

1 John J. Nelson (SBN 317598)
2 **MILBERG COLEMAN BRYSON**
3 **PHILLIPS GROSSMAN, LLC**
4 280 S. Beverly Drive
5 Beverly Hills, CA 90212
6 Telephone: (858) 209-6941
7 Email: jnelson@milberg.com

8 *Attorney for Plaintiff and the Proposed Class*

9
10 **UNITED STATES DISTRICT COURT**
CENTRAL DISTRICT OF CALIFORNIA

11 JAY GOLDSTEIN, individually and on
12 behalf of all others similarly situated,

13 Plaintiff,

14 vs.

15
16 PROSPECT MEDICAL HOLDINGS,
17 INC.,

18 Defendant.

Case No. _____

19
20 **CLASS ACTION COMPLAINT**

21 **JURY TRIAL DEMANDED**

22 Plaintiff Jay Goldstein (“Plaintiff”) brings this Class Action Complaint
23 (“Complaint”) against Defendant Prospect Medical Holdings, Inc. (“Prospect” or
24 “Defendant”) as an individual and on behalf of all others similarly situated, and
25 alleges, upon personal knowledge as to his own actions and his counsels’
26 investigation, and upon information and belief as to all other matters, as follows:

27 **NATURE OF THE ACTION**

1
2 1. Plaintiff brings this class action against Defendant for its failure to
3 properly secure and safeguard Plaintiff's and other similarly situated patients and/or
4 patients' sensitive information, including full names, dates of birth, and Social
5 Security numbers ("personally identifiable information" or "PII") and medical and
6 health insurance information, which is protected health information ("PHI", and
7 collectively with PII, "Private Information") as defined by the Health Insurance
8 Portability and Accountability Act of 1996 ("HIPAA").
9
10

11 2. Defendant is a healthcare corporation composed of "hospitals and
12 affiliated medical groups" that provide medical services to patients in "California,
13 Connecticut, Pennsylvania, Texas and Rhode Island."¹
14

15 3. Former and current patients of Defendant are required to entrust
16 Defendant with sensitive, non-public Private Information, in order to obtain medical
17 services from Defendant. Defendant retains this information for at least many years
18 and even after the relationship has ended.
19

20 4. By obtaining, collecting, using, and deriving a benefit from the Private
21 Information of Plaintiff and Class Members, Defendant assumed legal and equitable
22 duties to those individuals to protect and safeguard that information from
23 unauthorized access and intrusion.
24
25
26

27 ¹ <https://www.pmh.com/> (last accessed Oct. 12, 2023).
28

1 5. On August 1, 2023, Defendant "learned of a data security incident that
2 disrupted the operations of some of [its] IT systems."² In response, Defendant
3 "engaged the expertise of a third-party forensic investigation firm to conduct a
4 thorough investigation."³
5

6 6. According to Defendant's untitled letter sent to Plaintiff and Class
7 Members (the "Notice Letter"), the compromised Private Information included
8 individuals' names; dates of birth; Social Security numbers, diagnoses information,
9 lab results, prescription information, treatment information, and medical record
10 numbers.⁴
11

12 7. Defendant failed to adequately protect Plaintiff's and Class Members
13 Private Information—and failed to even encrypt or redact this highly sensitive
14 information. This unencrypted, unredacted Private Information was compromised
15 due to Defendant's negligent and/or careless acts and omissions and their utter failure
16 to protect Class Members' sensitive data. Hackers targeted and obtained Plaintiff's
17 and Class Members' Private Information because of its value in exploiting and
18
19
20
21
22
23

24 ² See Notice Letter. A sample copy is available at
25 <https://apps.web.maine.gov/online/aeviewer/ME/40/c4f1f925-6136-45dd-99fa-6c92cab12031.shtml> (last accessed Oct. 12, 2023).

26 ³ *Id.*

27 ⁴ *Id.*

1 stealing the identities of Plaintiff and Class Members. The present and continuing
2 risk to victims of the Data Breach will remain for their respective lifetimes.

3
4 8. Plaintiff brings this action on behalf of all persons whose Private
5 Information was compromised as a result of Defendant's failure to: (i) adequately
6 protect the Private Information of Plaintiff and Class Members; (ii) warn Plaintiff
7 and Class Members of Defendant's inadequate information security practices; and
8 (iii) effectively secure hardware containing protected Private Information using
9 reasonable and effective security procedures free of vulnerabilities and incidents.
10 Defendant's conduct amounts at least to negligence and violates federal and state
11 statutes.
12
13

14 9. Defendant disregarded the rights of Plaintiff and Class Members by
15 intentionally, willfully, recklessly, or negligently failing to implement and maintain
16 adequate and reasonable measures and ensure those measures were followed by its
17 IT vendors to ensure that the Private Information of Plaintiff and Class Members
18 was safeguarded, failing to take available steps to prevent an unauthorized disclosure
19 of data, and failing to follow applicable, required, and appropriate protocols,
20 policies, and procedures regarding the encryption of data, even for internal use. As
21 a result, the Private Information of Plaintiff and Class Members was compromised
22 through disclosure to an unknown and unauthorized third party. Plaintiff and Class
23
24
25
26
27
28

1 Members have a continuing interest in ensuring that their information is and remains
2 safe, and they should be entitled to injunctive and other equitable relief.

3
4 10. Plaintiff and Class Members have suffered injury as a result of
5 Defendant's conduct. These injuries include: (i) invasion of privacy; (ii) theft of their
6 Private Information; (iii) lost or diminished value of Private Information; (iv) lost
7 time and opportunity costs associated with attempting to mitigate the actual
8 consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost
9 opportunity costs associated with attempting to mitigate the actual consequences of
10 the Data Breach; (vii) experiencing an increase in spam calls, texts, and/or emails;
11 and (viii) the continued and certainly increased risk to their Private Information,
12 which: (a) remains unencrypted and available for unauthorized third parties to access
13 and abuse; and (b) remains backed up in Defendant's possession and is subject to
14 further unauthorized disclosures so long as Defendant fails to undertake appropriate
15 and adequate measures to protect the Private Information.

16
17 11. Plaintiff and Class Members seek to remedy these harms and prevent
18 any future data compromise on behalf of himself and all similarly situated persons
19 whose personal data was compromised and stolen as a result of the Data Breach and
20 who remain at risk due to Defendant's inadequate data security practices.

21 **PARTIES**

22 12. Plaintiff, Jay Goldstein, is a natural person and resident of Santa
23
24
25
26
27
28

1 Monica, California, where he intends to remain.

2 13. Defendant is a Delaware corporation with its principal place of
3 business located at 3415 South Sepulveda Boulevard, 9th Floor, Los Angeles,
4 California 90034.
5

6 **JURISDICTION AND VENUE**

7
8 14. This Court has subject matter jurisdiction over this action under 28
9 U.S.C. § 1332(d) because this is a class action wherein the amount in controversy
10 exceeds the sum or value of \$5,000,000, exclusive of interest and costs, there are
11 more than 100 members in the proposed class, and at least one member of the class
12 is a citizen of a state different from Defendant.⁵
13

14 15. This Court has personal jurisdiction over Defendant because its
15 principal place of business is in this District, regularly conducts business in
16 California, and the acts and omissions giving rise to Plaintiff's claims occurred in
17 and emanated from this District.
18
19

20 16. Venue is proper under 18 U.S.C. § 1391(b)(1) because Defendant's
21 principal place of business is in this District.
22

23 **FACTUAL ALLEGATIONS**

24
25
26 ⁵ According to the report submitted to the Office of the Maine Attorney General, 67 Maine
27 residents were impacted in the Data Breach. *See*
28 <https://apps.web.maine.gov/online/aevviewer/ME/40/c4f1f925-6136-45dd-99fa-6c92cab12031.shtml> (last accessed Oct. 12, 2023).

1 ***Defendant's Business***

2 17. Defendant is a healthcare corporation composed of “hospitals and
3 affiliated medical groups” that provide medical services to patients in “California,
4 Connecticut, Pennsylvania, Texas and Rhode Island.”⁶

5
6 18. Plaintiff and Class Members are current and former patients of
7 Defendant.
8

9 19. As a condition of receiving medical services at Prospect, Defendant
10 requires that its patients, including Plaintiff and Class Members, entrust it with
11 highly sensitive personal information.
12

13 20. The information held by Defendant in its computer systems or shared
14 with its vendors at the time of the Data Breach included the unencrypted Private
15 Information of Plaintiff and Class Members.
16

17 21. Upon information and belief, Defendant made promises and
18 representations to its patients, including Plaintiff and Class Members, that the
19 Private Information collected from them as a condition of obtaining medical
20 services at Prospect would be kept safe, confidential, that the privacy of that
21 information would be maintained, and that Defendant would delete any sensitive
22 information after it was no longer required to maintain it.
23
24

25 22. Indeed, Defendant's Privacy Statement provides that: “we have
26

27 ⁶ <https://www.pmh.com/> (last accessed Oct. 12, 2023).
28

1 security measures in place to protect against the loss, misuse and/or unauthorized
2 access of personal information . . . We aim to protect and keep confidential all
3 information that is voluntarily provided to us through this website[.]”⁷
4

5 23. Plaintiff and Class Members provided their Private Information to
6 Defendant, directly or indirectly, with the reasonable expectation and on the mutual
7 understanding that Defendant would comply with its obligations to keep such
8 information confidential and secure from unauthorized access.
9

10 24. Plaintiff and the Class Members have taken reasonable steps to
11 maintain the confidentiality of their Private Information. Plaintiff and Class
12 Members relied on the sophistication of Defendant to keep their Private
13 Information confidential and securely maintained, to use this information for
14 necessary purposes only, and to make only authorized disclosures of this
15 information. Plaintiff and Class Members value the confidentiality of their Private
16 Information and demand security to safeguard their Private Information.
17
18
19

20 25. Defendant had a duty to adopt reasonable measures to protect the
21 Private Information of Plaintiff and Class Members from involuntary disclosure to
22 third parties and to audit, monitor, and verify the integrity of its IT vendors’ and
23 affiliates’ data security practices and systems. Defendant has a legal duty to keep
24
25

26
27 ⁷ <https://www.pmh.com/globalassets/pmh/footer/pmhprivacypolicy.pdf> (last accessed Oct. 12,
28 2023).

1 patient's Private Information safe and confidential.

2 26. Defendant had obligations created by FTC Act, contract, industry
3 standards, and representations made to Plaintiff and Class Members, to keep their
4 Private Information confidential and to protect it from unauthorized access and
5 disclosure.
6

7 27. Defendant derived a substantial economic benefit from collecting
8 Plaintiff's and Class Members' Private Information. Without the required
9 submission of Private Information, Defendant could not perform the services it
10 provides.
11

12 28. By obtaining, collecting, using, and deriving a benefit from Plaintiff's
13 and Class Members' Private Information, Defendant assumed legal and equitable
14 duties and knew or should have known that it was responsible for protecting
15 Plaintiff's and Class Members' Private Information from disclosure.
16

17
18 ***The Data Breach***
19

20 29. On August 3, 2023 Defendant's network was breached by a well
21 known ransomware group called Rhysida.⁸ The Rhysida group previously rose to
22 prominence after exfiltrating and leaking data stolen from the Chilean Armed
23 Forces. The group has been so active that the Department of Health and Human
24

25
26
27 ⁸ <https://www.bleepingcomputer.com/news/security/rhysida-claims-ransomware-attack-on-prospect-medical-threatens-to-sell-data/>
28

Services published a bulletin outlining the group's mechanism of attack and advising health care organizations to take precautions against Rhysida.⁹ The HHS bulletin further warned that of the eight organizations attacked by Rhysida ransomware, the exfiltrated data was subsequently published from five of those organizations.¹⁰

30. Following the Data Breach, "[Rhysida] claim that they stole 1 TB of documents and a 1.3 TB SQL database containing 500,000 social security numbers, passports, driver's licenses, corporate documents, and patients' medical information."¹¹ The group also publicly posted "screenshots of driver's licenses, social security cards, documents, and what appears to be patients' medical information." The group demanded a payment of roughly \$1.3 million in exchange for the stolen information.

31. On or about September 29, 2023, Defendant began sending Plaintiff and other Data Breach victims an untitled letter (the "Notice Letter"), informing them that:

On August 1, 2023, Prospect Medical learned of a data security incident that disrupted the operations of some of our IT systems. We immediately took steps to secure our systems, contain the incident, and notify law enforcement. Additionally, we engaged the expertise of a third-party forensic investigation

⁹ <https://www.hhs.gov/sites/default/files/rhysida-ransomware-sector-alert-tlpclear.pdf>

¹⁰ *Id.*

¹¹ <https://www.bleepingcomputer.com/news/security/rhysida-claims-ransomware-attack-on-prospect-medical-threatens-to-sell-data/>

1 firm to conduct a thorough investigation.

2 Through our ongoing investigation, on September 13, 2023, we determined
3 that an unauthorized party gained access to our IT network between the dates
4 of July 31, 2023 and August 3, 2023. While in our IT network, the
5 unauthorized party accessed files that contain information pertaining to
6 Prospect Medical patients. Our investigation concluded that some of these
7 files contained your information, such as your name, Social Security number,
8 diagnosis information, lab results, prescription information, treatment
9 information, medical record number, and date of birth.¹²

10 32. Omitted from the Notice Letter were the details of the root cause of
11 the Data Breach, the vulnerabilities exploited, and the remedial measures
12 undertaken to ensure such a breach does not occur again. To date, these critical
13 facts have not been explained or clarified to Plaintiff and Class Members, who
14 retain a vested interest in ensuring that their Private Information remains protected.

15 33. This “disclosure” amounts to no real disclosure at all, as it fails to
16 inform, with any degree of specificity, Plaintiff and Class Members of the Data
17 Breach’s critical facts. Without these details, Plaintiff’s and Class Members’ ability
18 to mitigate the harms resulting from the Data Breach is severely diminished.

19 34. A ransomware attack, like that experienced by Defendants is a type of
20 cyberattack that is frequently used to target companies due to the sensitive patient
21 data they maintain.¹³ In a ransomware attack the attackers use software to encrypt
22 data they maintain.¹³ In a ransomware attack the attackers use software to encrypt
23 data they maintain.¹³ In a ransomware attack the attackers use software to encrypt
24 data they maintain.¹³ In a ransomware attack the attackers use software to encrypt

25 ¹² The Notice Letter.

26 ¹³ *Ransomware warning: Now attacks are stealing data as well as encrypting it*, available at
27 <https://www.zdnet.com/article/ransomware-warning-now-attacks-are-stealing-data-as-well-as-encrypting-it/>
28

1 data on a compromised network, rendering it unusable and demanding payment to
2 restore control over the network.¹⁴

3
4 35. Companies should treat ransomware attacks as any other data breach
5 incident because ransomware attacks don't just hold networks hostage,
6 "ransomware groups sell stolen data in cybercriminal forums and dark web
7 marketplaces for additional revenue."¹⁵ As cybersecurity expert Emisoft warns,
8 "[a]n absence of evidence of exfiltration should not be construed to be evidence of
9 its absence [...] the initial assumption should be that data may have been
10 exfiltrated."
11
12

13 36. An increasingly prevalent form of ransomware attack is the
14 "encryption+exfiltration" attack in which the attacker encrypts a network and
15 exfiltrates the data contained within.¹⁶ In 2020, over 50% of ransomware attackers
16 exfiltrated data from a network before encrypting it.¹⁷ Once the data is exfiltrated
17 from a network, its confidential nature is destroyed and it should be "assume[d] it
18 will be traded to other threat actors, sold, or held for a second/future extortion
19
20
21

22 ¹⁴ *Ransomware: The Data Exfiltration and Double Extortion Trends*, available at
23 <https://www.cisecurity.org/insights/blog/ransomware-the-data-exfiltration-and-double-extortion-trends>

24 ¹⁵ *The chance of data being stolen in a ransomware attack is greater than one in ten*, available at
25 <https://blog.emsisoft.com/en/36569/the-chance-of-data-being-stolen-in-a-ransomware-attack-is-greater-than-one-in-ten/>

26 ¹⁶ *2020 Ransomware Marketplace Report*, available at <https://www.coveware.com/blog/q3-2020-ransomware-marketplace-report>

27 ¹⁷ *Ransomware FAQs*, available at <https://www.cisa.gov/stopransomware/ransomware-faqs>

1 attempt.”¹⁸ And even where companies pay for the return of data attackers often
2 leak or sell the data regardless because there is no way to verify copies of the data
3 are destroyed.¹⁹
4

5 37. The attacker accessed and acquired files Defendant shared with a third
6 party containing unencrypted Private Information of Plaintiff and Class Members,
7 including their Social Security numbers, PHI, and other sensitive information.
8 Plaintiff’s and Class Members’ Private Information was accessed and stolen in the
9 Data Breach.
10

11 38. Plaintiff believes that his Private Information and that of Class
12 Members was subsequently sold on the dark web following the Data Breach, as that
13 is the *modus operandi* of cybercriminals that commit cyber-attacks of this type.
14
15

16 ***Data Breaches Are Preventable***

17 39. Defendant could have prevented this Data Breach by, among other
18 things, properly encrypting Private Information being shared with its vendors or
19 otherwise ensuring that such Private Information was protected while in transit or
20 accessible.
21

22 40. Defendant did not use reasonable security procedures and practices
23 appropriate to the nature of the sensitive information they were maintaining for
24
25

26 ¹⁸ *Id.*

27 ¹⁹ *Id.*

1 Plaintiff and Class Members, causing the exposure of Private Information, such as
2 encrypting the information or deleting it when it is no longer needed.

3
4 41. The unencrypted Private Information of Class Members will end up
5 for sale to identity thieves on the dark web, if it has not already, or it could simply
6 fall into the hands of companies that will use the detailed Private Information for
7 targeted marketing without the approval of Plaintiff and Class Members.
8 Unauthorized individuals can easily access the Private Information of Plaintiff and
9 Class Members.
10

11
12 42. As explained by the Federal Bureau of Investigation, “[p]revention is
13 the most effective defense against ransomware and it is critical to take precautions
14 for protection.”²⁰
15

16 43. To prevent and detect ransomware attacks Defendant could and should
17 have implemented, as recommended by the United States Government, the
18 following measures:
19

- 20 ● Implement an awareness and training program. Because end users are
21 targets, patients and individuals should be aware of the threat of
22 ransomware and how it is delivered.
- 23 ● Enable strong spam filters to prevent phishing emails from reaching the
24 end users and authenticate inbound email using technologies like Sender
25 Policy Framework (SPF), Domain Message Authentication Reporting

26 ²⁰ See How to Protect Your Networks from RANSOMWARE, at 3, available at
27 <https://www.fbi.gov/file-repository/ransomware-prevention-and-response-for-cisos.pdf/view>
28 (last visited Aug. 23, 2021).

1 and Conformance (DMARC), and DomainKeys Identified Mail (DKIM)
2 to prevent email spoofing.

- 3 ● Scan all incoming and outgoing emails to detect threats and filter
4 executable files from reaching end users.
- 5 ● Configure firewalls to block access to known malicious IP addresses.
- 6 ● Patch operating systems, software, and firmware on devices. Consider
7 using a centralized patch management system.
- 8 ● Set anti-virus and anti-malware programs to conduct regular scans
9 automatically.
- 10 ● Manage the use of privileged accounts based on the principle of least
11 privilege: no users should be assigned administrative access unless
12 absolutely needed; and those with a need for administrator accounts
13 should only use them when necessary.
- 14 ● Configure access controls—including file, directory, and network share
15 permissions—with least privilege in mind. If a user only needs to read
16 specific files, the user should not have write access to those files,
17 directories, or shares.
- 18 ● Disable macro scripts from office files transmitted via email. Consider
19 using Office Viewer software to open Microsoft Office files transmitted
20 via email instead of full office suite applications.
- 21 ● Implement Software Restriction Policies (SRP) or other controls to
22 prevent programs from executing from common ransomware locations,
23 such as temporary folders supporting popular Internet browsers or
24 compression/decompression programs, including the
AppData/LocalAppData folder.
- 25 ● Consider disabling Remote Desktop protocol (RDP) if it is not being
26 used.

- Use application whitelisting, which only allows systems to execute programs known and permitted by security policy.
- Execute operating system environments or specific programs in a virtualized environment.
- Categorize data based on organizational value and implement physical and logical separation of networks and data for different organizational units.²¹

44. To prevent and detect cyber-attacks or ransomware attacks Defendant could and should have implemented, as recommended by the Microsoft Threat Protection Intelligence Team, the following measures:

Secure internet-facing assets

- Apply latest security updates
- Use threat and vulnerability management
- Perform regular audit; remove privileged credentials;

Thoroughly investigate and remediate alerts

- Prioritize and treat commodity malware infections as potential full compromise;

Include IT Pros in security discussions

- Ensure collaboration among [security operations], [security admins], and [information technology] admins to configure servers and other endpoints securely;

Build credential hygiene

- Use [multifactor authentication] or [network level authentication] and use strong, randomized, just-in-time local admin passwords;

²¹ *Id.* at 3-4.

Apply principle of least-privilege

- Monitor for adversarial activities
- Hunt for brute force attempts
- Monitor for cleanup of Event Logs
- Analyze logon events;

Harden infrastructure

- Use Windows Defender Firewall
- Enable tamper protection
- Enable cloud-delivered protection
- Turn on attack surface reduction rules and [Antimalware Scan Interface] for Office[Visual Basic for Applications].²²

45. Given that Defendant was storing the Private Information of its current and former patients, Defendant could and should have implemented all of the above measures to prevent and detect cyberattacks.

Defendant Acquires, Collects, And Stores Patients' Private Information

46. Defendant has historically acquired, collected, stored, and shared the Private Information of Plaintiff and Class Members.

47. As a condition of obtaining medical services at Prospect, Defendant requires that its patients entrust it with highly sensitive personal information.

48. By obtaining, collecting, sharing, and using Plaintiff's and Class Members' Private Information, Defendant assumed legal and equitable duties and knew or should have known that it was responsible for protecting Plaintiff's and

²² See Human-operated ransomware attacks: A preventable disaster (Mar 5, 2020), *available at*: <https://www.microsoft.com/security/blog/2020/03/05/human-operated-ransomware-attacks-a-preventable-disaster/> (last visited Nov. 11, 2021).

1 Class Members' Private Information from disclosure.

2 49. Plaintiff and the Class Members have taken reasonable steps to
3
4 maintain the confidentiality of their Private Information.

5 50. Defendant could have prevented this Data Breach by properly
6 securing and encrypting the files and file servers containing the Private Information
7
8 of Plaintiff and Class Members or by exercising due diligence in selecting its IT
9 vendors and properly auditing those vendor's security practices.

10 51. Upon information and belief, Defendant made promises to Plaintiff
11 and Class Members to maintain and protect their Private Information,
12 demonstrating an understanding of the importance of securing Private Information.
13

14 52. Indeed, Defendant's Privacy Statement provides that: "we have
15 security measures in place to protect against the loss, misuse and/or unauthorized
16 access of personal information . . . We aim to protect and keep confidential all
17 information that is voluntarily provided to us through this website[.]"²³
18

19
20 53. Plaintiff and the Class Members relied on Defendant to keep their
21 Private Information confidential and securely maintained, to use this information
22 for business purposes only, and to make only authorized disclosures of this
23 information.
24

25 ***Defendant Knew or Should Have Known of the Risk Because Healthcare***

26
27 ²³ <https://www.pmh.com/globalassets/pmh/footer/pmhprivacypolicy.pdf> (last accessed Oct. 12,
28 2023).

Entities In Possession Of Private Information Are Particularly Susceptible To Cyber Attacks

54. Defendant's data security obligations were particularly important given the substantial increase in cyber-attacks and/or data breaches targeting health care entities that collect and store Private Information, like Defendant, preceding the date of the breach.

55. Data thieves regularly target companies like Defendant's due to the highly sensitive information that they custody. Defendant knew and understood that unprotected Private Information is valuable and highly sought after by criminal parties who seek to illegally monetize that Private Information through unauthorized access.

56. In the third quarter of the 2023 fiscal year alone, 7333 organizations experienced data breaches, resulting in 66,658,764 individuals' personal information being compromised.²⁴

57. In light of recent high profile cybersecurity incidents at other healthcare partner and provider companies, including American Medical Collection Agency (25 million patients and/or patients, March 2019), University of Washington Medicine (974,000 patients and/or patients, December 2018), Florida Orthopedic Institute (640,000 patients and/or patients, July 2020), Wolverine

²⁴ See <https://www.idtheftcenter.org/publication/q3-data-breach-2023-analysis/> (last accessed Oct. 11, 2023).

1 Solutions Group (600,000 patients and/or patients, September 2018), Oregon
2 Department of Human Services (645,000 patients and/or patients, March 2019),
3 Elite Emergency Physicians (550,000 patients and/or patients, June 2020),
4 Magellan Health (365,000 patients and/or patients, April 2020), and BJC Health
5 System (286,876 patients and/or patients, March 2020), Defendant knew or should
6 have known that its electronic records would be targeted by cybercriminals
7
8

9 58. As a custodian of Private Information, Defendant knew, or should
10 have known, the importance of safeguarding the Private Information entrusted to it
11 by Plaintiff and Class members, and of the foreseeable consequences if its data
12 security systems were breached, including the significant costs imposed on Plaintiff
13 and Class Members as a result of a breach.
14
15

16 59. Indeed, cyberattacks have become so notorious that the Federal
17 Bureau of Investigation (“FBI”) and U.S. Secret Service have issued a warning to
18 potential targets so they are aware of, and prepared for, a potential attack. As one
19 report explained, “[e]ntities like smaller municipalities and hospitals are attractive
20 to ransomware criminals . . . because they often have lesser IT defenses and a high
21 incentive to regain access to their data quickly.”²⁵
22
23

24 60. Despite the prevalence of public announcements of data breach and
25

26 ²⁵ FBI, Secret Service Warn of Targeted, Law360 (Nov. 18, 2019),
27 <https://www.law360.com/articles/1220974/fbisecret-service-warn-of-targeted-ransomware> (last
28 visited Sep. 13, 2022).

1 data security compromises, Defendant failed to take appropriate steps to protect the
2 Private Information of Plaintiff and Class Members from being compromised.
3

4 61. At all relevant times, Defendant knew, or reasonably should have
5 known, of the importance of safeguarding the Private Information of Plaintiff and
6 Class Members and of the foreseeable consequences that would occur if
7 Defendant's data security system was breached, including, specifically, the
8 significant costs that would be imposed on Plaintiff and Class Members as a result
9 of a breach.
10

11
12 62. Defendant was, or should have been, fully aware of the unique type
13 and the significant volume of data on Defendant's server(s), amounting to over one
14 hundred thousand individuals' detailed, Private Information, and, thus, the
15 significant number of individuals who would be harmed by the exposure of the
16 unencrypted data.
17

18
19 63. Additionally, as companies became more dependent on computer
20 systems to run their business,²⁶ e.g., working remotely as a result of the Covid-19
21 pandemic, and the Internet of Things ("IoT"), the danger posed by cybercriminals
22 is magnified, thereby highlighting the need for adequate administrative, physical,
23
24
25

26
27 ²⁶<https://www.federalreserve.gov/econres/notes/feds-notes/implications-of-cyber-risk-for-financial-stability-20220512.html>
28

1 and technical safeguards.²⁷

2 64. In the Notice Letter, Defendant offers to provide 12 months of credit
3 monitoring and identity theft insurance services. This is wholly inadequate to
4 compensate Plaintiff and Class Members as it fails to provide for the fact victims
5 of data breaches and other unauthorized disclosures commonly face multiple years
6 of ongoing identity theft, financial fraud, and it entirely fails to provide sufficient
7 compensation for the unauthorized release and disclosure of Plaintiff and Class
8 Members' Private Information. Moreover, once this service expires, Plaintiff and
9 Class Members will be forced to pay out of pocket for necessary identity
10 monitoring services.
11
12
13

14 65. Defendant's offer of credit and identity monitoring establishes that
15 Plaintiff's and Class Members' sensitive Private Information *was* in fact affected,
16 accessed, compromised, and exfiltrated from Defendant's computer systems.
17
18

19 66. The injuries to Plaintiff and Class Members were directly and
20 proximately caused by Defendant's failure to implement or maintain adequate data
21 security measures for the Private Information of Plaintiff and Class Members.
22

23 67. The ramifications of Defendant's failure to keep secure the Private
24 Information of Plaintiff and Class Members are long lasting and severe. Once
25
26

27 ²⁷ <https://www.picussecurity.com/key-threats-and-cyber-risks-facing-financial-services-and-banking-firms-in-2022>
28

1 Private Information is stolen—particularly Social Security numbers and PHI—
2 fraudulent use of that information and damage to victims may continue for years.

3
4 68. As a healthcare entity in possession of sensitive Private Information,
5 Defendant knew, or should have known, the importance of safeguarding the Private
6 Information entrusted to them by Plaintiff and Class Members and of the
7 foreseeable consequences if its data security systems were breached. This includes
8 the significant costs imposed on Plaintiff and Class Members as a result of a breach.
9 Nevertheless, Defendant failed to take adequate cybersecurity measures to prevent
10 the Data Breach.
11

12
13 ***Defendant Fails To Comply With FTC Guidelines***

14 69. The Federal Trade Commission (“FTC”) has promulgated numerous
15 guides for businesses which highlight the importance of implementing reasonable
16 data security practices. According to the FTC, the need for data security should be
17 factored into all business decision-making.
18

19
20 70. In 2016, the FTC updated its publication, Protecting Personal
21 Information: A Guide for Business, which established cyber-security guidelines for
22 businesses. These guidelines note that businesses should protect the personal
23 patient information that they keep; properly dispose of personal information that is
24 no longer needed; encrypt information stored on computer networks; understand
25 their network’s vulnerabilities; and implement policies to correct any security
26
27
28

1 problems.²⁸

2 71. The guidelines also recommend that businesses use an intrusion
3 detection system to expose a breach as soon as it occurs; monitor all incoming
4 traffic for activity indicating someone is attempting to hack the system; watch for
5 large amounts of data being transmitted from the system; and have a response plan
6 ready in the event of a breach.²⁹
7

8 72. The FTC further recommends that companies not maintain Private
9 Information longer than is needed for authorization of a transaction; limit access to
10 sensitive data; require complex passwords to be used on networks; use industry-
11 tested methods for security; monitor for suspicious activity on the network; and
12 verify that third-party service providers have implemented reasonable security
13 measures.
14

15 73. The FTC has brought enforcement actions against healthcare
16 companies for failing to protect patient data adequately and reasonably, treating the
17 failure to employ reasonable and appropriate measures to protect against
18 unauthorized access to confidential patient data as an unfair act or practice
19 prohibited by Section 5 of the Federal Trade Commission Act (“FTCA”), 15 U.S.C.
20
21
22
23
24

25 ²⁸ *Protecting Personal Information: A Guide for Business*, Federal Trade Commission (2016).
26 Available at [https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-](https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf)
27 [personal-information.pdf](https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf) (last visited Oct. 17, 2022).

28 ²⁹ *Id.*

1 § 45. Orders resulting from these actions further clarify the measures businesses
2 must take to meet their data security obligations.

3
4 74. These FTC enforcement actions include actions against healthcare
5 companies, like Defendant. *See, e.g., In the Matter of LabMD, Inc., A Corp*, 2016-
6 2 Trade Cas. (Henry Ford) ¶ 79708, 2016 WL 4128215, at *32 (MSNET July 28,
7 2016) (“[T]he Commission concludes that LabMD’s data security practices were
8 unreasonable and constitute an unfair act or practice in violation of Section 5 of the
9 FTC Act.”).

10
11
12 75. Defendant failed to properly implement basic data security practices.

13 76. Defendant’s failure to employ reasonable and appropriate measures to
14 protect against unauthorized access to patients’ Private Information constitutes an
15 unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

16
17 77. Upon information and belief, Defendant was at all times fully aware
18 of its obligation to protect the Private Information of its patients. Defendant was
19 also aware of the significant repercussions that would result from its failure to do
20 so.
21

22 ***Defendant Fails to Comply with HIPAA Guidelines***

23
24 78. Defendant is a covered business associate under HIPAA (45 C.F.R. §
25 160.102) and is required to comply with the HIPAA Privacy Rule and Security
26 Rule, 45 C.F.R. Part 160 and Part 164, Subparts A and E (“Standards for Privacy
27
28

1 of Individually Identifiable Health Information”), and Security Rule (“Security
2 Standards for the Protection of Electronic Protected Health Information”), 45
3 C.F.R. Part 160 and Part 164, Subparts A and C.

5 79. Defendant is subject to the rules and regulations for safeguarding
6 electronic forms of medical information pursuant to the Health Information
7 Technology Act (“HITECH”).³⁰ See 42 U.S.C. §17921, 45 C.F.R. § 160.103.

9 80. HIPAA’s Privacy Rule or *Standards for Privacy of Individually*
10 *Identifiable Health Information* establishes national standards for the protection of
11 health information.

13 81. HIPAA’s Privacy Rule or *Security Standards for the Protection of*
14 *Electronic Protected Health Information* establishes a national set of security
15 standards for protecting health information that is kept or transferred in electronic
16 form.

18 82. HIPAA requires “compl[iance] with the applicable standards,
19 implementation specifications, and requirements” of HIPAA “with respect to
20 electronic protected health information.” 45 C.F.R. § 164.302.

22 83. “Electronic protected health information” is “individually identifiable
23 health information ... that is (i) transmitted by electronic media; maintained in
24

26
27 ³⁰ HIPAA and HITECH work in tandem to provide guidelines and rules for maintaining
28 protected health information. HITECH references and incorporates HIPAA.

1 electronic media.” 45 C.F.R. § 160.103.

2 84. HIPAA’s Security Rule requires Defendant to do the following:

- 3 a. Ensure the confidentiality, integrity, and availability of all
4 electronic protected health information the covered entity or
5 business associate creates, receives, maintains, or transmits;
6
7 b. Protect against any reasonably anticipated threats or hazards to
8 the security integrity of such information;
9
10 c. Protect against any reasonably anticipated uses or disclosures of
11 such information that are not permitted; and
12
13 d. Ensure compliance by its workforce.

14 85. HIPAA also requires Defendant to “review and modify the security
15 measures implemented ... as needed to continue provision of reasonable and
16 appropriate protection of electronic protected health information.” 45 C.F.R. §
17 164.306(e). Additionally, Defendant is required under HIPAA to “[i]mplement
18 technical policies and procedures for electronic information systems that maintain
19 electronic protected health information to allow access only to those persons or
20 software programs that have been granted access rights.” 45 C.F.R. §
21 164.312(a)(1).
22
23
24

25 86. HIPAA and HITECH also obligated Defendant to implement policies
26 and procedures to prevent, detect, contain, and correct security violations, and to
27
28

1 protect against uses or disclosures of electronic protected health information that
2 are reasonably anticipated but not permitted by the privacy rules. *See* 45 C.F.R. §
3 164.306(a)(1) and § 164.306(a)(3); *see also* 42 U.S.C. §17902.

5 87. The HIPAA Breach Notification Rule, 45 C.F.R. §§ 164.400-414, also
6 requires Defendant to provide notice of the Data Breach to each affected individual
7 “without unreasonable delay and *in no case later than 60 days following discovery*
8 *of the breach.*”³¹

10 88. HIPAA requires a covered entity to have and apply appropriate
11 sanctions against members of its workforce who fail to comply with the privacy
12 policies and procedures of the covered entity or the requirements of 45 C.F.R. Part
13 164, Subparts D or E. *See* 45 C.F.R. § 164.530(e).

16 89. HIPAA requires a covered entity to mitigate, to the extent practicable,
17 any harmful effect that is known to the covered entity of a use or disclosure of
18 protected health information in violation of its policies and procedures or the
19 requirements of 45 C.F.R. Part 164, Subpart E by the covered entity or its business
20 associate. *See* 45 C.F.R. § 164.530(f).

22 90. HIPAA also requires the Office of Civil Rights (“OCR”), within the
23 Department of Health and Human Services (“HHS”), to issue annual guidance
24

26
27 ³¹ Breach Notification Rule, U.S. Dep’t of Health & Human Services,
28 <https://www.hhs.gov/hipaa/for-professionals/breach-notification/index.html> (emphasis added).

1 documents on the provisions in the HIPAA Security Rule. *See* 45 C.F.R. §§
2 164.302-164.318. For example, “HHS has developed guidance and tools to assist
3 HIPAA covered entities in identifying and implementing the most cost effective
4 and appropriate administrative, physical, and technical safeguards to protect the
5 confidentiality, integrity, and availability of e-PHI and comply with the risk
6 analysis requirements of the Security Rule.” US Department of Health & Human
7 Services, Security Rule Guidance Material.³² The list of resources includes a link
8 to guidelines set by the National Institute of Standards and Technology (NIST),
9 which OCR says “represent the industry standard for good business practices with
10 respect to standards for securing e-PHI.” US Department of Health & Human
11 Services, Guidance on Risk Analysis.³³

12
13
14
15
16 ***Defendant Fails To Comply With Industry Standards***

17 91. As noted above, experts studying cyber security routinely identify
18 healthcare companies in possession of Private Information as being particularly
19 vulnerable to cyberattacks because of the value of the Private Information which
20 they collect and maintain.

21
22 92. Several best practices have been identified that, at a minimum, should
23
24
25

26 ³² <http://www.hhs.gov/hipaa/for-professionals/security/guidance/index.html>.

27 ³³ [https://www.hhs.gov/hipaa/for-professionals/security/guidance/guidance-risk-](https://www.hhs.gov/hipaa/for-professionals/security/guidance/guidance-risk-analysis/index.html)
28 [analysis/index.html](https://www.hhs.gov/hipaa/for-professionals/security/guidance/guidance-risk-analysis/index.html)

1 be implemented by healthcare companies in possession of Private Information, like
2 Defendant, including but not limited to: educating all patients; strong passwords;
3 multi-layer security, including firewalls, anti-virus, and anti-malware software;
4 encryption, making data unreadable without a key; multi-factor authentication;
5 backup data and limiting which patients can access sensitive data. Defendant failed
6 to follow these industry best practices, including a failure to implement multi-factor
7 authentication.
8
9

10 93. Other best cybersecurity practices that are standard in the healthcare
11 industry include installing appropriate malware detection software; monitoring and
12 limiting the network ports; protecting web browsers and email management
13 systems; setting up network systems such as firewalls, switches and routers;
14 monitoring and protection of physical security systems; protection against any
15 possible communication system; training staff regarding critical points. Defendant
16 failed to follow these cybersecurity best practices, including failure to train staff.
17
18
19

20 94. Defendant failed to meet the minimum standards of any of the
21 following frameworks: the NIST Cybersecurity Framework Version 1.1 (including
22 without limitation PR.AC-1, PR.AC-3, PR.AC-4, PR.AC-5, PR.AC-6, PR.AC-7,
23 PR.AT-1, PR.DS-1, PR.DS-5, PR.PT-1, PR.PT-3, DE.CM-1, DE.CM-4, DE.CM-
24 7, DE.CM-8, and RS.CO-2), and the Center for Internet Security's Critical Security
25 Controls (CIS CSC), which are all established standards in reasonable
26
27
28

1 cybersecurity readiness.

2 95. These foregoing frameworks are existing and applicable industry
3 standards in the healthcare industry, and upon information and belief, Defendant
4 failed to comply with at least one—or all—of these accepted standards, thereby
5 opening the door to the threat actor and causing the Data Breach.
6

7
8 ***Defendant's Breach***

9 96. Defendant breached its obligations to Plaintiff and Class Members
10 and/or was otherwise negligent and reckless by conducting the following acts
11 and/or omissions:
12

- 13 a. Failing to maintain an adequate data security system to reduce the risk
14 of data breaches and cyber-attacks;
15
16 b. Failing to adequately protect Private Information;
17
18 c. Failing to ensure the confidentiality and integrity of electronic Private
19 Information it created, received, maintained, and/or transmitted;
20
21 d. Failing to implement technical policies and procedures for electronic
22 information systems that maintain electronic Private Information to
23 allow access only to those persons or software programs that have been
24 granted access rights;
25
26 e. Failing to implement policies and procedures to prevent, detect,
27 contain, and correct security violations;
28

- f. Failing to implement procedures to review records of information system activity regularly, such as audit logs, access reports, and security incident tracking reports;
- g. Failing to protect against reasonably anticipated threats or hazards to the security or integrity of electronic Private Information;
- h. Failing to train all members of their workforces effectively on the policies and procedures regarding Private Information;
- i. Failing to render the electronic Private Information it maintained unusable, unreadable, or indecipherable to unauthorized individuals;
- j. Failing to comply with FTC guidelines for cybersecurity, in violation of Section 5 of the FTC Act;
- k. Failing to audit, monitor, and verify the adequacy of its vendors' data security practices
- l. Failing to adhere to HIPAA guidelines and industry standards for cybersecurity as discussed above; and,
- m. Otherwise breaching their duties and obligations to protect Plaintiff's and Class Members' Private Information.

97. Defendant negligently and unlawfully failed to safeguard Plaintiff's and Class Members' Private Information by allowing cyberthieves to access Defendant's online insurance application flow, which provided unauthorized actors

1 with unsecured and unencrypted Private Information.

2 98. Had Defendant remedied the deficiencies in its information storage
3 and security systems or those of its vendors and affiliates, followed industry
4 guidelines, and adopted security measures recommended by experts in the field, it
5 could have prevented intrusion into its information storage and security systems
6 and, ultimately, the theft of Plaintiff's and Class Members' confidential Private
7 Information.
8

9 99. Accordingly, as outlined below, Plaintiff and Class Members now face
10 a present, increased risk of fraud and identity theft. In addition, Plaintiff and the
11 Class Members lost the benefit of the bargain they made with Defendant.
12

13 **COMMON INJURIES & DAMAGES**
14

15 100. As a result of Defendant's ineffective and inadequate data security
16 practices, the Data Breach, and the foreseeable consequences of Private
17 Information ending up in the possession of criminals, the risk of identity theft to
18 the Plaintiff and Class Members has materialized and is imminent, and Plaintiff and
19 Class Members have all sustained actual injuries and damages, including: (a)
20 invasion of privacy; (b) loss of time and loss of productivity incurred mitigating the
21 materialized risk and imminent threat of identity theft risk; (c) the loss of benefit of
22 the bargain (price premium damages); (d) diminution of value of their Private
23 Information; (e) invasion of privacy; and (f) the continued risk to their Private
24
25
26
27
28

1 Information, which remains in the possession of Defendant, and which is subject to
2 further breaches, so long as Defendant fails to undertake appropriate and adequate
3 measures to protect Plaintiff's and Class Members' Private Information.
4

5 ***The Data Breach Increases Victims' Risk Of Identity Theft***

6 101. Plaintiff and Class Members are at a heightened risk of identity theft
7 for years to come.
8

9 102. The unencrypted Private Information of Class Members will end up
10 for sale on the dark web because that is the *modus operandi* of hackers. In addition,
11 unencrypted Private Information may fall into the hands of companies that will use
12 the detailed Private Information for targeted marketing without the approval of
13 Plaintiff and Class Members. Unauthorized individuals can easily access the
14 Private Information of Plaintiff and Class Members.
15
16

17 103. The link between a data breach and the risk of identity theft is simple
18 and well established. Criminals acquire and steal Private Information to monetize
19 the information. Criminals monetize the data by selling the stolen information on
20 the black market to other criminals who then utilize the information to commit a
21 variety of identity theft related crimes discussed below.
22
23

24 104. Because a person's identity is akin to a puzzle with multiple data
25 points, the more accurate pieces of data an identity thief obtains about a person, the
26 easier it is for the thief to take on the victim's identity--or track the victim to attempt
27
28

1 other hacking crimes against the individual to obtain more data to perfect a crime.

2 105. For example, armed with just a name and date of birth, a data thief can
3
4 utilize a hacking technique referred to as “social engineering” to obtain even more
5 information about a victim’s identity, such as a person’s login credentials or Social
6 Security number. Social engineering is a form of hacking whereby a data thief uses
7
8 previously acquired information to manipulate and trick individuals into disclosing
9 additional confidential or personal information through means such as spam phone
10 calls and text messages or phishing emails. Data Breaches can be the starting point
11
12 for these additional targeted attacks on the victim.

13 106. One such example of criminals piecing together bits and pieces of
14 compromised Private Information for profit is the development of “Fullz”
15
16 packages.³⁴

17 107. With “Fullz” packages, cyber-criminals can cross-reference two
18

19 ³⁴ “Fullz” is fraudster speak for data that includes the information of the victim, including, but
20 not limited to, the name, address, credit card information, social security number, date of birth,
21 and more. As a rule of thumb, the more information you have on a victim, the more money that
22 can be made off of those credentials. Fullz are usually pricier than standard credit card
23 credentials, commanding up to \$100 per record (or more) on the dark web. Fullz can be cashed
24 out (turning credentials into money) in various ways, including performing bank transactions
25 over the phone with the required authentication details in-hand. Even “dead Fullz,” which are
26 Fullz credentials associated with credit cards that are no longer valid, can still be used for
27 numerous purposes, including tax refund scams, ordering credit cards on behalf of the victim, or
28 opening a “mule account” (an account that will accept a fraudulent money transfer from a
compromised account) without the victim’s knowledge. *See, e.g.,* Brian Krebs, *Medical Records
for Sale in Underground Stolen From Texas Life Insurance Firm*, Krebs on Security (Sep. 18,
2014), [https://krebsonsecurity.com/2014/09/medical-records-for-sale-in-underground-stolen-](https://krebsonsecurity.com/2014/09/medical-records-for-sale-in-underground-stolen-from-texas-life-insurance-/)
[https://krebsonsecurity.com/2014/09/medical-records-for-sale-in-](https://krebsonsecurity.com/2014/09/medical-records-for-sale-in-underground-stolen-from-texas-life-insurance-finn/)
[underground-stolen-from-texas-life-insurance-finn/](https://krebsonsecurity.com/2014/09/medical-records-for-sale-in-underground-stolen-from-texas-life-insurance-finn/) (last visited on May 26, 2023).

1 sources of Private Information to marry unregulated data available elsewhere to
2 criminally stolen data with an astonishingly complete scope and degree of accuracy
3
4 in order to assemble complete dossiers on individuals.

5 108. The development of “Fullz” packages means here that the stolen
6 Private Information from the Data Breach can easily be used to link and identify it
7
8 to Plaintiff’ and Class Members’ phone numbers, email addresses, and other
9 unregulated sources and identifiers. In other words, even if certain information such
10 as emails, phone numbers, or credit card numbers may not be included in the Private
11 Information that was exfiltrated in the Data Breach, criminals may still easily create
12 a Fullz package and sell it at a higher price to unscrupulous operators and criminals
13 (such as illegal and scam telemarketers) over and over.
14
15

16 109. The existence and prevalence of “Fullz” packages means that the
17 Private Information stolen from the data breach can easily be linked to the
18 unregulated data (like phone numbers and emails) of Plaintiff and the other Class
19 Members.
20

21 110. Thus, even if certain information (such as driver's license numbers)
22 was not stolen in the data breach, criminals can still easily create a comprehensive
23 “Fullz” package.
24

25 111. Then, this comprehensive dossier can be sold—and then resold in
26 perpetuity—to crooked operators and other criminals (like illegal and scam
27
28

1 telemarketers).

2 ***Loss Of Time To Mitigate Risk Of Identity Theft And Fraud***

3
4 112. As a result of the recognized risk of identity theft, when a Data Breach
5 occurs, and an individual is notified by a company that their Private Information
6 was compromised, as in this Data Breach, the reasonable person is expected to take
7 steps and spend time to address the dangerous situation, learn about the breach, and
8 otherwise mitigate the risk of becoming a victim of identity theft of fraud. Failure
9 to spend time taking steps to review accounts or credit reports could expose the
10 individual to greater financial harm – yet, the resource and asset of time has been
11 lost.
12
13

14 113. Thus, due to the actual and imminent risk of identity theft, Plaintiff
15 and Class Members must monitor their financial accounts for many years to
16 mitigate the risk of identity theft. The Notice Letter sent by Defendant to Plaintiff
17 and Class Members encourages them to take “some additional steps you can take
18 in response, please see the additional information provided in this letter.”³⁵
19
20

21 114. Plaintiff and Class Members have spent, and will spend additional
22 time in the future, on a variety of prudent actions, such as researching and verifying
23 the legitimacy of the Data Breach upon receiving the Notice Letter, signing up for
24 the credit and identity theft monitoring services offered by Defendant, and checking
25
26

27 ³⁵ Notice Letter.
28

1 their financial accounts for any indication of fraudulent activity, which may take
2 years to detect..

3
4 115. Plaintiff's mitigation efforts are consistent with the U.S. Government
5 Accountability Office that released a report in 2007 regarding data breaches ("GAO
6 Report") in which it noted that victims of identity theft will face "substantial costs
7 and time to repair the damage to their good name and credit record."³⁶
8

9 116. Plaintiff's mitigation efforts are also consistent with the steps that FTC
10 recommends that data breach victims take several steps to protect their personal
11 and financial information after a data breach, including: contacting one of the credit
12 bureaus to place a fraud alert (consider an extended fraud alert that lasts for seven
13 years if someone steals their identity), reviewing their credit reports, contacting
14 companies to remove fraudulent charges from their accounts, placing a credit freeze
15 on their credit, and correcting their credit reports.³⁷
16
17

18 ***Diminution Value Of Private Information***
19

20 117. PII and PHI are valuable property rights.³⁸ Their value is axiomatic,
21

22 ³⁶ See United States Government Accountability Office, GAO-07-737, Personal Information:
23 Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the
24 Full Extent Is Unknown (June 2007), <https://www.gao.gov/new.items/d07737.pdf>.

25 ³⁷ See Federal Trade Commission, *Identity Theft.gov*, <https://www.identitytheft.gov/Steps> (last
26 visited July 7, 2022).

27 ³⁸ See, e.g., Randall T. Soma, et al, Corporate Privacy Trend: The "Value" of Personally
28 Identifiable Information ("Private Information") Equals the "Value" of Financial Assets, 15
Rich. J.L. & Tech. 11, at *3-4 (2009) ("Private Information, which companies obtain at little

1 considering the value of Big Data in corporate America and the consequences of
2 cyber thefts include heavy prison sentences. Even this obvious risk to reward
3 analysis illustrates beyond doubt that Private Information has considerable market
4 value.
5

6 118. An active and robust legitimate marketplace for PII exists. In 2019,
7
8 the data brokering industry was worth roughly \$200 billion.³⁹

9 119. In fact, the data marketplace is so sophisticated that consumers can
10 actually sell their non-public information directly to a data broker who in turn
11 aggregates the information and provides it to marketers or app developers.^{40,41}
12

13 120. Consumers who agree to provide their web browsing history to the
14 Nielsen Corporation can receive up to \$50.00 a year.⁴²
15

16 121. Conversely sensitive PII can sell for as much as \$363 per record on
17 the dark web according to the Infosec Institute.⁴³
18

19 122. Theft of PHI is also gravely serious: “[a] thief may use your name or
20

21 cost, has quantifiable value that is rapidly reaching a level comparable to the value of traditional
22 financial assets.”) (citations omitted).

23 ³⁹ <https://www.latimes.com/business/story/2019-11-05/column-data-brokers>

24 ⁴⁰ <https://datacoup.com/>

25 ⁴¹ <https://digi.me/what-is-digime/>

26 ⁴² Nielsen Computer & Mobile Panel, Frequently Asked Questions, available at
27 <https://computermobilepanel.nielsen.com/ui/US/en/fagen.html>

28 ⁴³ See Ashiq Ja, *Hackers Selling Healthcare Data in the Black Market*, InfoSec (July 27, 2015),
<https://resources.infosecinstitute.com/topic/hackers-selling-healthcare-data-in-the-black-market/>
(last visited Sep. 13, 2022).

1 health insurance numbers to see a doctor, get prescription drugs, file claims with
2 your insurance provider, or get other care. If the thief's health information is mixed
3 with yours, your treatment, insurance and payment records, and credit report may
4 be affected.”

6 123. According to account monitoring company LogDog, medical data
7 sells for \$50 and up on the Dark Web.⁴⁴

9 124. As a result of the Data Breach, Plaintiff's and Class Members' Private
10 Information, which has an inherent market value in both legitimate and dark
11 markets, has been damaged and diminished by its compromise and unauthorized
12 release. However, this transfer of value occurred without any consideration paid to
13 Plaintiff or Class Members for their property, resulting in an economic loss.
14 Moreover, the Private Information is now readily available, and the rarity of the
15 Data has been lost, thereby causing additional loss of value.

18 125. Based on the foregoing, the information compromised in the Data
19 Breach is significantly more valuable than the loss of, for example, credit card
20 information in a retailer data breach because, there, victims can cancel or close
21 credit and debit card accounts. The information compromised in this Data Breach
22 is impossible to “close” and difficult, if not impossible, to change, e.g., names,
23
24

26 ⁴⁴ Lisa Vaas, *Ransomware Attacks Paralyze, and Sometimes Crush, Hospitals*, Naked Security
27 (Oct. 3, 2019), <https://nakedsecurity.sophos.com/2019/10/03/ransomware-attacks-paralyze-and-sometimes-crush-hospitals/#content> (last accessed July 20, 2021)

1 Social Security numbers,, PHI, and dates of birth.

2 126. Among other forms of fraud, identity thieves may obtain driver's
3 licenses, government benefits, medical services, and housing or even give false
4 information to police.
5

6 127. The fraudulent activity resulting from the Data Breach may not come
7 to light for years.
8

9 128. At all relevant times, Defendant knew, or reasonably should have
10 known, of the importance of safeguarding the Private Information of Plaintiff and
11 Class Members, and of the foreseeable consequences that would occur if
12 Defendant's data security system was breached, including, specifically, the
13 significant costs that would be imposed on Plaintiff and Class Members as a result
14 of a breach.
15
16

17 129. Defendant was, or should have been, fully aware of the unique type
18 and the significant volume of data on Defendant's network, amounting to over one
19 hundred thousands individuals' detailed personal information, upon information
20 and belief, and thus, the significant number of individuals who would be harmed
21 by the exposure of the unencrypted data.
22
23

24 130. The injuries to Plaintiff and Class Members were directly and
25 proximately caused by Defendant's failure to implement or maintain adequate data
26 security measures for the Private Information of Plaintiff and Class Members.
27
28

Future Cost of Credit and Identity Theft Monitoring is Reasonable and Necessary

131. Given the type of targeted attack in this case and sophisticated criminal activity, the type of Private Information involved, and the volume of data obtained in the Data Breach, there is a strong probability that entire batches of stolen information have been placed, or will be placed, on the black market/dark web for sale and purchase by criminals intending to utilize the Private Information for identity theft crimes –e.g., opening bank accounts in the victims’ names to make purchases or to launder money; file false tax returns; take out loans or lines of credit; or file false unemployment claims.

132. Such fraud may go undetected until debt collection calls commence months, or even years, later. An individual may not know that his or her Social Security Number was used to file for unemployment benefits until law enforcement notifies the individual’s employer of the suspected fraud. Fraudulent tax returns are typically discovered only when an individual’s authentic tax return is rejected.

133. Furthermore, the information accessed and disseminated in the Data Breach is significantly more valuable than the loss of, for example, credit card information in a retailer data breach, where victims can easily cancel or close credit and debit card accounts.⁴⁵ The information disclosed in this Data Breach is

⁴⁵ See Jesse Damiani, *Your Social Security Number Costs \$4 On The Dark Web*, New Report

1 impossible to “close” and difficult, if not impossible, to change (such as Social
2 Security numbers).

3
4 134. Consequently, Plaintiff and Class Members are at a present and
5 continuous risk of fraud and identity theft for many years into the future.

6 135. The retail cost of credit monitoring and identity theft monitoring can
7 cost around \$200 a year per Class Member. This is reasonable and necessary cost
8 to monitor to protect Class Members from the risk of identity theft that arose from
9 Defendant’s Data Breach.
10

11
12 ***Loss Of The Benefit Of The Bargain***

13 136. Furthermore, Defendant’s poor data security deprived Plaintiff and
14 Class Members of the benefit of their bargain. When obtaining medical services at
15 Defendant under certain terms, Plaintiff and other reasonable patients understood
16 and expected that they were, in part, paying, or being paid less, for services and
17 data security to protect the Private Information, when in fact, Defendant did not
18 provide the expected data security. Accordingly, Plaintiff and Class Members
19 received medical services that were of a lesser value than what they reasonably
20 expected to receive under the bargains they struck with Defendant.
21
22
23

24 **PLAINTIFF GOLDSTEIN'S EXPERIENCE**

25
26
27

Finds, FORBES (Mar. 25, 2020), <https://www.forbes.com/sites/jessedamiani/2020/03/25/your-social-security-number-costs-4-on-the-dark-web-new-report-finds/?sh=6a44b6d513f1>.
28

1 137. Plaintiff Jay Goldstein is a former Prosect patient that obtained
2 medical services at Defendant in or about 2020.

3
4 138. As a condition obtaining medical services at Prospect, Plaintiff was
5 required to provide his Private Information to Defendant, including his name, date
6 of birth, and Social Security number.

7
8 139. At the time of the Data Breach—July 31, 2023 through August 3,
9 2023—Defendant retained Plaintiff’s Private Information in its system.

10 140. Plaintiff Jay Goldstein is very careful about sharing his sensitive
11 Private Information. Plaintiff stores any documents containing his Private
12 Information in a safe and secure location. He has never knowingly transmitted
13 unencrypted sensitive Private Information over the internet or any other unsecured
14 source. Plaintiff would not have entrusted his Private Information to Defendant had
15 he known of Defendant’s lax data security policies.

16
17
18 141. Plaintiff Jay Goldstein received the Notice Letter, by U.S. mail,
19 directly from Defendant, dated September 29, 2023. According to the Notice Letter,
20 Plaintiff’s Private Information was improperly accessed and obtained by
21 unauthorized third parties, including his name, Social Security number, diagnosis
22 information, lab results, prescription information, treatment information, medical
23 record number, and date of birth.

24
25
26 142. As a result of the Data Breach, and at the direction of Defendant’s
27
28

1 Notice Letter, Plaintiff made reasonable efforts to mitigate the impact of the Data
2 Breach, including researching and verifying the legitimacy of the Data Breach upon
3 receiving the Notice Letter, signing up for the credit and identity theft monitoring
4 services offered by Defendant, and checking his financial accounts for any
5 indication of fraudulent activity, which may take years to detect.. Plaintiff has spent
6 significant time dealing with the Data Breach, valuable time Plaintiff otherwise
7 would have spent on other activities, including but not limited to work and/or
8 recreation. This time has been lost forever and cannot be recaptured.
9
10

11
12 143. Plaintiff suffered actual injury from having his Private Information
13 compromised as a result of the Data Breach including, but not limited to: (i)
14 invasion of privacy; (ii) theft of his Private Information; (iii) lost or diminished
15 value of Private Information; (iv) lost time and opportunity costs associated with
16 attempting to mitigate the actual consequences of the Data Breach; (v) loss of
17 benefit of the bargain; (vi) lost opportunity costs associated with attempting to
18 mitigate the actual consequences of the Data Breach; and (vii) the continued and
19 certainly increased risk to his Private Information, which: (a) remains unencrypted
20 and available for unauthorized third parties to access and abuse; and (b) remains
21 backed up in Defendant's possession and is subject to further unauthorized
22 disclosures so long as Defendant fails to undertake appropriate and adequate
23 measures to protect the Private Information.
24
25
26
27
28

1 144. Plaintiff further suffered actual injury in the form of experiencing an
2 increase in spam calls, texts, and/or emails, which, upon information and belief,
3 was caused by the Data Breach.
4

5 145. The Data Breach has caused Plaintiff to suffer fear, anxiety, and stress,
6 which has been compounded by the fact that Defendant has still not fully informed
7 him of key details about the Data Breach's occurrence.
8

9 146. As a result of the Data Breach, Plaintiff anticipates spending
10 considerable time and money on an ongoing basis to try to mitigate and address
11 harms caused by the Data Breach.
12

13 147. As a result of the Data Breach, Plaintiff is at a present risk and will
14 continue to be at increased risk of identity theft and fraud for years to come.
15

16 148. Plaintiff Jay Goldstein has a continuing interest in ensuring that his
17 Private Information, which, upon information and belief, remains backed up in
18 Defendant's possession, is protected and safeguarded from future breaches.
19

20 **CLASS ACTION ALLEGATIONS**

21 149. This action is properly maintainable as a class action. Plaintiff brings
22 this class action on behalf of himself and on behalf of all others similarly situated.
23

24 150. Plaintiff proposes the following Class definitions, subject to
25 amendment as appropriate:
26

27 **Nationwide Class**

28 All individuals residing in the United States whose Private Information was

1 compromised in the data breach announced by Defendant in September 2023
2 (the “Class”).

3 **California Subclass**

4 All individuals residing in the state of California whose Private Information
5 was compromised in the data breach announced by Defendant in September
6 2023 (the “California Subclass”).

7 151. Excluded from the Classes are the following individuals and/or entities:
8 Defendant and Defendant’s parents, subsidiaries, affiliates, officers and directors,
9 and any entity in which Defendant has a controlling interest; all individuals who
10 make a timely election to be excluded from this proceeding using the correct protocol
11 for opting out; and all judges assigned to hear any aspect of this litigation, as well as
12 their immediate family members.
13

14 152. Numerosity: The members of the Class are so numerous that joinder of
15 all members is impracticable, if not completely impossible. At least 190,000
16 individuals were notified by Defendant of the Data Breach, according to the breach
17 report submitted to Office of the Maine Attorney General.⁴⁶ The Class is apparently
18 identifiable within Defendant’s records, and Defendant has already identified these
19 individuals (as evidenced by sending them breach notification letters).
20
21

22 153. Common questions of law and fact exist as to all members of the Class
23 that predominate over any questions affecting solely individual members of the
24
25

26 _____
27 ⁴⁶ <https://apps.web.maine.gov/online/aewiewer/ME/40/c4f1f925-6136-45dd-99fa-6c92cab12031.shtml> (last accessed Oct. 12, 2023).
28

1 Class. The questions of law and fact common to the Class, which may affect
2 individual Class members, include, but are not limited to, the following:

- 3 a. Whether and to what extent Defendant had a duty to protect the
4 Private Information of Plaintiff and Class Members;
- 5 b. Whether Defendant had respective duties not to disclose the Private
6 Information of Plaintiff and Class Members to unauthorized third
7 parties;
- 8 c. Whether Defendant had respective duties not to use the Private
9 Information of Plaintiff and Class Members for non-business
10 purposes;
- 11 d. Whether Defendant failed to adequately safeguard the Private
12 Information of Plaintiff and Class Members;
- 13 e. Whether and when Defendant actually learned of the Data Breach;
- 14 f. Whether Defendant adequately, promptly, and accurately informed
15 Plaintiff and Class Members that their Private Information had been
16 compromised;
- 17 g.. Whether Defendant violated the law by failing to promptly notify
18 Plaintiff and Class Members that their Private Information had been
19 compromised;
- 20 h. Whether Defendant failed to implement and maintain reasonable
21
22
23
24
25
26
27
28

1 security procedures and practices appropriate to the nature and scope
2 of the information compromised in the Data Breach;

3
4 i. Whether Defendant adequately addressed and fixed the
5 vulnerabilities which permitted the Data Breach to occur;

6 j. Whether Plaintiff and Class Members are entitled to actual damages,
7 statutory damages, and/or nominal damages as a result of Defendant's
8 wrongful conduct; and
9

10 k. Whether Plaintiff and Class Members are entitled to injunctive relief
11 to redress the imminent and currently ongoing harm faced as a result
12 of the Data Breach.
13

14 154. Typicality: Plaintiff's claims are typical of those of the other members
15 of the Class because Plaintiff, like every other Class Member, was exposed to
16 virtually identical conduct and now suffers from the same violations of the law as
17 each other member of the Class.
18

19
20 155. Policies Generally Applicable to the Class: This class action is also
21 appropriate for certification because Defendant acted or refused to act on grounds
22 generally applicable to the Class, thereby requiring the Court's imposition of
23 uniform relief to ensure compatible standards of conduct toward the Class Members
24 and making final injunctive relief appropriate with respect to the Nationwide Class
25 as a whole. Defendant's policies challenged herein apply to and affect Class
26
27
28

1 Members uniformly and Plaintiff's challenge of these policies hinges on Defendant's
2 conduct with respect to the Class as a whole, not on facts or law applicable only to
3 Plaintiff.
4

5 156. Adequacy: Plaintiff will fairly and adequately represent and protect the
6 interests of the Class Members in that he has no disabling conflicts of interest that
7 would be antagonistic to those of the other Class Members. Plaintiff seeks no relief
8 that is antagonistic or adverse to the Class Members and the infringement of the
9 rights and the damages he has suffered are typical of other Class Members. Plaintiff
10 has retained counsel experienced in complex class action and data breach litigation,
11 and Plaintiff intends to prosecute this action vigorously.
12
13

14 157. Superiority and Manageability: The class litigation is an appropriate
15 method for fair and efficient adjudication of the claims involved. Class action
16 treatment is superior to all other available methods for the fair and efficient
17 adjudication of the controversy alleged herein; it will permit a large number of Class
18 Members to prosecute their common claims in a single forum simultaneously,
19 efficiently, and without the unnecessary duplication of evidence, effort, and expense
20 that hundreds of individual actions would require. Class action treatment will permit
21 the adjudication of relatively modest claims by certain Class Members, who could
22 not individually afford to litigate a complex claim against large corporations, like
23 Defendant. Further, even for those Class Members who could afford to litigate such
24
25
26
27
28

1 a claim, it would still be economically impractical and impose a burden on the courts.

2 158. The nature of this action and the nature of laws available to Plaintiff
3 and Class Members make the use of the class action device a particularly efficient
4 and appropriate procedure to afford relief to Plaintiff and Class Members for the
5 wrongs alleged because Defendant would necessarily gain an unconscionable
6 advantage since they would be able to exploit and overwhelm the limited resources
7 of each individual Class Member with superior financial and legal resources; the
8 costs of individual suits could unreasonably consume the amounts that would be
9 recovered; proof of a common course of conduct to which Plaintiff was exposed is
10 representative of that experienced by the Class and will establish the right of each
11 Class Member to recover on the cause of action alleged; and individual actions
12 would create a risk of inconsistent results and would be unnecessary and duplicative
13 of this litigation.

14 159. The litigation of the claims brought herein is manageable. Defendant's
15 uniform conduct, the consistent provisions of the relevant laws, and the ascertainable
16 identities of Class Members demonstrates that there would be no significant
17 manageability problems with prosecuting this lawsuit as a class action.

18 160. Adequate notice can be given to Class Members directly using
19 information maintained in Defendant's records.

20 161. Unless a Class-wide injunction is issued, Defendant may continue in its
21
22
23
24
25
26
27
28

1 failure to properly secure the Private Information of Class Members, Defendant may
2 continue to refuse to provide proper notification to Class Members regarding the
3 Data Breach, and Defendant may continue to act unlawfully as set forth in this
4 Complaint.
5

6 162. Further, Defendant has acted or refused to act on grounds generally
7 applicable to the Class and, accordingly, final injunctive or corresponding
8 declaratory relief with regard to the Class Members as a whole is appropriate under
9 Code of Civil Procedure § 382.
10

11
12 **COUNT I**
13 **Negligence**
14 **(On Behalf of Plaintiff and the Class)**

15 163. Plaintiff restates and realleges the preceding factual allegations set forth
16 above as if fully alleged herein.

17 164. Defendant requires its patients, including Plaintiff and Class Members,
18 to submit non-public Private Information in the ordinary course of providing its
19 medical services.
20

21 165. Defendant gathered and stored the Private Information of Plaintiff and
22 Class Members as part of its business of soliciting its services to its patients, which
23 solicitations and services affect commerce.
24

25 166. Plaintiff and Class Members entrusted Defendant with their Private
26 Information with the understanding that Defendant would safeguard their
27
28

1 information.

2 167. Defendant had full knowledge of the sensitivity of the Private
3 Information and the types of harm that Plaintiff and Class Members could and would
4 suffer if the Private Information were wrongfully disclosed.
5

6 168. By assuming the responsibility to collect and store this data, and in fact
7 doing so, and sharing it and using it for commercial gain, Defendant had a duty of
8 care to use reasonable means to secure and safeguard their computer property—and
9 Class Members' Private Information held within it—to prevent disclosure of the
10 information, and to safeguard the information from theft. Defendant's duty included
11 a responsibility to implement processes by which they could detect a breach of its
12 security systems in a reasonably expeditious period of time and to give prompt notice
13 to those affected in the case of a data breach.
14
15
16

17 169. Defendant had a duty to employ reasonable security measures under
18 Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, which prohibits
19 "unfair . . . practices in or affecting commerce," including, as interpreted and
20 enforced by the FTC, the unfair practice of failing to use reasonable measures to
21 protect confidential data.
22
23

24 170. Defendant's duty to use reasonable security measures under HIPAA
25 required Defendant to "reasonably protect" confidential data from "any intentional
26 or unintentional use or disclosure" and to "have in place appropriate administrative,
27
28

1 technical, and physical safeguards to protect the privacy of protected health
2 information." 45 C.F.R. § 164.530(c)(l). Some or all of the healthcare and/or medical
3 information at issue in this case constitutes "protected health information" within the
4 meaning of HIPAA.
5

6 171. Defendant owed a duty of care to Plaintiff and Class Members to
7 provide data security consistent with industry standards and other requirements
8 discussed herein, and to ensure that its systems and networks, and the personnel
9 responsible for them, adequately protected the Private Information.
10

11 172. Defendant's duty of care to use reasonable security measures arose as
12 a result of the special relationship that existed between Defendant and its patients.
13 That special relationship arose because Plaintiff and the Class entrusted Defendant
14 with their confidential Private Information, a necessary part of being patients of
15 Defendant.
16

17 173. Defendant's duty to use reasonable care in protecting confidential data
18 arose not only as a result of the statutes and regulations described above, but also
19 because Defendant is bound by industry standards to protect confidential Private
20 Information.
21

22 174. Defendant was subject to an "independent duty," untethered to any
23 contract between Defendant and Plaintiff or the Class.
24

25 175. Defendant also had a duty to exercise appropriate clearinghouse
26
27
28

1 practices to remove former patients' Private Information it was no longer required
2 to retain pursuant to regulations.

3
4 176. Moreover, Defendant had a duty to promptly and adequately notify
5 Plaintiff and the Class of the Data Breach.

6
7 177. Defendant had and continues to have a duty to adequately disclose that
8 the Private Information of Plaintiff and the Class within Defendant's possession
9 might have been compromised, how it was compromised, and precisely the types of
10 data that were compromised and when. Such notice was necessary to allow Plaintiff
11 and the Class to take steps to prevent, mitigate, and repair any identity theft and the
12 fraudulent use of their Private Information by third parties.

13
14 178. Defendant breached its duties, pursuant to the FTC Act, HIPAA, and
15 other applicable standards, and thus were negligent, by failing to use reasonable
16 measures to protect Class Members' Private Information. The specific negligent acts
17 and omissions committed by Defendant include, but are not limited to, the following:
18

- 19
20 a. Failing to adopt, implement, and maintain adequate security measures
21 to safeguard Class Members' Private Information;
22
23 b. Failing to adequately monitor the security of their networks and
24 systems;
25
26 c. Failure to periodically ensure that their email system had plans in place
27 to maintain reasonable data security safeguards;
28

- d. Allowing unauthorized access to Class Members' Private Information;
- e. Failing to detect in a timely manner that Class Members' Private Information had been compromised;
- f. Failing to remove former patients' Private Information it was no longer required to retain pursuant to regulations,
- g. Failing to timely and adequately notify Class Members about the Data Breach's occurrence and scope, so that they could take appropriate steps to mitigate the potential for identity theft and other damages;
- h. Failing to audit, monitor, and verify the adequacy of its vendors' security practices; and
- i. Failing to secure its stand-alone personal computers, such as the reception desk computers, even after discovery of the data breach.

179. Defendant violated Section 5 of the FTC Act and HIPAA by failing to use reasonable measures to protect Private Information and not complying with applicable industry standards, as described in detail herein. Defendant's conduct was particularly unreasonable given the nature and amount of Private Information it obtained and stored and the foreseeable consequences of the immense damages that would result to Plaintiff and the Class.

180. Plaintiff and the Class are within the class of persons that the FTC Act and HIPAA were intended to protect.

1 181. The harm that occurred as a result of the Data Breach is the type of
2 harm the FTC Act and HIPAA were intended to guard against.

3
4 182. Defendant's violation of Section 5 of the FTC Act and HIPAA
5 constitutes negligence.

6 183. The FTC has pursued enforcement actions against businesses, which,
7 as a result of their failure to employ reasonable data security measures and avoid
8 unfair and deceptive practices, caused the same harm as that suffered by Plaintiff
9 and the Class.
10

11
12 184. A breach of security, unauthorized access, and resulting injury to
13 Plaintiff and the Class was reasonably foreseeable, particularly in light of
14 Defendant's inadequate security practices.
15

16 185. It was foreseeable that Defendant's failure to use reasonable measures
17 to protect Class Members' Private Information would result in injury to Class
18 Members. Further, the breach of security was reasonably foreseeable given the
19 known high frequency of cyberattacks and data breaches in the healthcare industry.
20

21 186. Defendant has full knowledge of the sensitivity of the Private
22 Information and the types of harm that Plaintiff and the Class could and would suffer
23 if the Private Information were wrongfully disclosed.
24

25 187. Plaintiff and the Class were the foreseeable and probable victims of any
26 inadequate security practices and procedures. Defendant knew or should have
27
28

1 known of the inherent risks in collecting and storing the Private Information of
2 Plaintiff and the Class, the critical importance of providing adequate security of that
3 Private Information, and the necessity for encrypting Private Information stored on
4 Defendant's systems.
5

6 188. It was therefore foreseeable that the failure to adequately safeguard
7 Class Members' Private Information would result in one or more types of injuries to
8 Class Members.
9

10 189. Plaintiff and the Class had no ability to protect their Private Information
11 that was in, and possibly remains in, Defendant's possession.
12

13 190. Defendant was in a position to protect against the harm suffered by
14 Plaintiff and the Class as a result of the Data Breach.
15

16 191. Defendant's duty extended to protecting Plaintiff and the Class from
17 the risk of foreseeable criminal conduct of third parties, which has been recognized
18 in situations where the actor's own conduct or misconduct exposes another to the
19 risk or defeats protections put in place to guard against the risk, or where the parties
20 are in a special relationship. *See* Restatement (Second) of Torts § 302B. Numerous
21 courts and legislatures have also recognized the existence of a specific duty to
22 reasonably safeguard personal information.
23
24

25 192. Defendant has admitted that the Private Information of Plaintiff and the
26 Class was wrongfully lost and disclosed to unauthorized third persons as a result of
27
28

1 the Data Breach.

2 193. But for Defendant's wrongful and negligent breach of duties owed to
3 Plaintiff and the Class, the Private Information of Plaintiff and the Class would not
4 have been compromised.
5

6 194. There is a close causal connection between Defendant's failure to
7 implement security measures to protect the Private Information of Plaintiff and the
8 Class and the harm, or risk of imminent harm, suffered by Plaintiff and the Class.
9 The Private Information of Plaintiff and the Class was lost and accessed as the
10 proximate result of Defendant's failure to exercise reasonable care in safeguarding
11 such Private Information by adopting, implementing, and maintaining appropriate
12 security measures.
13
14
15

16 195. As a direct and proximate result of Defendant's negligence, Plaintiff
17 and the Class have suffered and will suffer injury, including but not limited to: (i)
18 invasion of privacy; (ii) theft of their Private Information; (iii) lost or diminished
19 value of Private Information; (iv) lost time and opportunity costs associated with
20 attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit
21 of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the
22 actual consequences of the Data Breach; (vii) experiencing an increase in spam calls,
23 texts, and/or emails; and (viii) the continued and certainly increased risk to their
24 Private Information, which: (a) remains unencrypted and available for unauthorized
25
26
27
28

1 third parties to access and abuse; and (b) remains backed up in Defendant's
2 possession and is subject to further unauthorized disclosures so long as Defendant
3 fails to undertake appropriate and adequate measures to protect the Private
4 Information.
5

6 196. As a direct and proximate result of Defendant's negligence, Plaintiff
7 and the Class have suffered and will continue to suffer other forms of injury and/or
8 harm, including, but not limited to, anxiety, emotional distress, loss of privacy, and
9 other economic and non-economic losses.
10

11 197. Additionally, as a direct and proximate result of Defendant's
12 negligence, Plaintiff and the Class have suffered and will suffer the continued risks
13 of exposure of their Private Information, which remain in Defendant's possession
14 and is subject to further unauthorized disclosures so long as Defendant fails to
15 undertake appropriate and adequate measures to protect the Private Information in
16 its continued possession.
17
18

19 198. Plaintiff and Class Members are entitled to compensatory and
20 consequential damages suffered as a result of the Data Breach.
21

22 199. Defendant's negligent conduct is ongoing, in that it still holds the
23 Private Information of Plaintiff and Class Members in an unsafe and insecure
24 manner.
25

26 200. Plaintiff and Class Members are also entitled to injunctive relief
27
28

1 requiring Defendant to (i) strengthen its data security systems and monitoring
2 procedures; (ii) submit to future annual audits of those systems and monitoring
3 procedures; and (iii) continue to provide adequate credit monitoring to all Class
4 Members.
5

6
7 **COUNT II**
8 **Breach Of Implied Contract**
9 **(On Behalf of Plaintiff and the Class)**

10 201. Plaintiff restates and realleges the preceding factual allegations set forth
11 above as if fully alleged herein.

12 202. Plaintiff and Class Members were required to provide their Private
13 Information to Defendant as a condition of receiving medical services from
14 Defendant.
15

16 203. Plaintiff and the Class entrusted their Private Information to Defendant.
17 In so doing, Plaintiff and the Class entered into implied contracts with Defendant by
18 which Defendant agreed to safeguard and protect such information, to keep such
19 information secure and confidential, and to timely and accurately notify Plaintiff and
20 the Class if their data had been breached and compromised or stolen.
21

22 204. Implicit in the agreement between Plaintiff and Class Members and the
23 Defendant to provide Private Information, was the latter's obligation to: (a) use such
24 Private Information for business purposes only, (b) take reasonable steps to
25 safeguard that Private Information, (c) prevent unauthorized disclosures of the
26
27
28

1 Private Information, (d) provide Plaintiff and Class Members with prompt and
2 sufficient notice of any and all unauthorized access and/or theft of their Private
3 Information, (e) reasonably safeguard and protect the Private Information of Plaintiff
4 and Class Members from unauthorized disclosure or uses, (f) retain the Private
5 Information only under conditions that kept such information secure and
6 confidential.
7
8

9 205. The mutual understanding and intent of Plaintiff and Class Members on
10 the one hand, and Defendant, on the other, is demonstrated by their conduct and
11 course of dealing.
12

13 206. Defendant solicited, offered, and invited Plaintiff and Class Members
14 to provide their Private Information as part of Defendant's regular business
15 practices. Plaintiff and Class Members accepted Defendant's offers and provided
16 their Private Information to Defendant.
17

18 207. In accepting the Private Information of Plaintiff and Class Members,
19 Defendant understood and agreed that it was required to reasonably safeguard the
20 Private Information from unauthorized access or disclosure.
21

22 208. On information and belief, at all relevant times Defendant promulgated,
23 adopted, and implemented written privacy policies whereby it expressly promised
24 Plaintiff and Class Members that it would only disclose Private Information under
25 certain circumstances, none of which relate to the Data Breach.
26
27
28

1 209. On information and belief, Defendant further promised to comply with
2 industry standards and to make sure that Plaintiff's and Class Members' Private
3 Information would remain protected.
4

5 210. In entering into such implied contracts, Plaintiff and Class Members
6 reasonably believed and expected that Defendant's data security practices complied
7 with relevant laws and regulations and were consistent with industry standards.
8

9 211. Plaintiff and Class Members paid money to Defendant with the
10 reasonable belief and expectation that Defendant would use part of its earnings to
11 obtain adequate data security. Defendant failed to do so.
12

13 212. Plaintiff and Class Members would not have entrusted their Private
14 Information to Defendant in the absence of the implied contract between them and
15 Defendant to keep their information reasonably secure.
16

17 213. Plaintiff and Class Members would not have entrusted their Private
18 Information to Defendant in the absence of their implied promise to monitor their
19 computer systems and networks to ensure that it adopted reasonable data security
20 measures.
21

22 214. Plaintiff and Class Members fully and adequately performed their
23 obligations under the implied contracts with Defendant.
24

25 215. Defendant breached the implied contracts it made with Plaintiff and the
26 Class by failing to safeguard and protect their personal information, by failing to
27
28

1 delete the information of Plaintiff and the Class once the relationship ended, and by
2 failing to provide accurate notice to them that personal information was
3 compromised as a result of the Data Breach.
4

5 216. As a direct and proximate result of Defendant's breach of the implied
6 contracts, Plaintiff and Class Members sustained damages, as alleged herein,
7 including the loss of the benefit of the bargain.
8

9 217. Plaintiff and Class Members are entitled to compensatory,
10 consequential, and nominal damages suffered as a result of the Data Breach.
11

12 218. Plaintiff and Class Members are also entitled to injunctive relief
13 requiring Defendant to, *e.g.*, (i) strengthen its data security systems and monitoring
14 procedures; (ii) submit to future annual audits of those systems and monitoring
15 procedures; and (iii) immediately provide adequate credit monitoring to all Class
16 Members.
17

18
19 **COUNT III**
20 **Unjust Enrichment / Quasi Contract**
(On Behalf of Plaintiff and the Class)

21 219. Plaintiff restates and realleges the preceding factual allegations set forth
22 above as if fully alleged herein.
23

24 220. This Count is pleaded in the alternative to the breach of implied contract
25 claim (Count II) above.
26

27 221. Plaintiff and Class Members conferred a monetary benefit upon
28

1 Defendant in the form of providing their valuable Private Information to Defendant.

2 222. Plaintiff and Class Members provided Defendant their Private
3
4 Information on the understanding that Defendant would pay for the administrative
5 costs of reasonable data privacy and security practices and procedures from the
6 revenue it derived therefrom. In exchange, Plaintiff and Class Members should have
7
8 received adequate protection and data security for such Private Information held by
9 Defendant.

10 223. Defendant benefited from receiving Plaintiff's and Class Members'
11
12 labor and from receiving their Private Information through its ability to retain and
13 use that information for its own benefit. Defendant understood and accepted this
14 benefit.

15
16 224. Defendant knew Plaintiff and Class members conferred a benefit which
17 Defendant accepted. Defendant profited from these transactions and used the Private
18 Information of Plaintiff and Class Members for business purposes.

19
20 225. Because all Private Information provided by Plaintiff and Class
21 Members was similarly at risk from a foreseeable and targeted data breach,
22 Defendant's obligation to safeguard the Private Information it collected from its
23 patients was inherent to the relationship.

24
25 226. Defendant also understood and appreciated that Plaintiff's and Class
26 Members' Private Information was private and confidential, and its value depended
27
28

1 upon Defendant maintaining the privacy and confidentiality of that information.

2 227. Defendant failed to provide reasonable security, safeguards, and
3
4 protections to the Private Information of Plaintiff and Class Members.

5 228. Defendant enriched itself by saving the costs it reasonably should have
6 expended on data security measures to secure Plaintiff' and Class Members' Private
7
8 Information.

9 229. Instead of providing a reasonable level of security that would have
10 prevented the Data Breach, Defendant instead made calculated decisions to avoid its
11 data security obligations at the expense of Plaintiff and Class Members by utilizing
12 cheaper, ineffective security measures. Plaintiff and Class Members, on the other
13 hand, suffered as a direct and proximate result of Defendant's failure to provide the
14 requisite security.
15
16

17 230. Under the principles of equity and good conscience, Defendant should
18 not be permitted to retain money belonging to Plaintiff and Class Members, because
19 Defendant failed to implement appropriate data management and security measures
20 mandated by industry standards.
21

22 231. Defendant's enrichment at the expense of Plaintiff and Class Members
23 is and was unjust.
24

25 232. Defendant acquired the monetary benefit and Private Information
26 through inequitable means in that they failed to disclose the inadequate security
27
28

1 practices previously alleged.

2 233. If Plaintiff and Class Members knew that Defendant had not secured
3 their Private Information, they would not have agreed to provide their Private
4 Information to Defendant.
5

6 234. Plaintiff and Class Members have no adequate remedy at law.
7

8 235. As a direct and proximate result of Defendant's conduct, Plaintiff and
9 Class Members have suffered and will suffer injury as described herein.
10

11 236. Plaintiff and the Class Members are entitled to restitution and
12 disgorgement of all profits, benefits, and other compensation obtained by Defendant,
13 plus attorneys' fees, costs, and interest thereon.
14

15 **COUNT IV**
16 **Violation of the California Unfair Competition Law,**
17 **Cal. Bus. & Prof. Code §17200 *et seq.***
(On Behalf of Plaintiff and the California Subclass)

18 237. Plaintiff re-alleges and incorporates by reference each and every
19 allegation in this Complaint, as if fully set forth herein.
20

21 238. Defendant is a "person" defined by Cal. Bus. & Prof. Code § 17201.

22 239. Defendant violated Cal. Bus. & Prof. Code § 17200 *et seq.* ("UCL") by
23 engaging in unlawful, unfair, and deceptive business acts and practices.
24

25 240. Defendant's "unfair" acts and practices include:

- 26 a. Defendant failed to implement and maintain reasonable security
27 measures to protect Plaintiff's and California Subclass Members'
28

1 personal information from unauthorized disclosure, release, data
2 breaches, and theft, which was a direct and proximate cause of the
3 Defendant Data Breach. Defendant failed to identify foreseeable
4 security risks, remediate identified security risks, and adequately
5 improve security following previous cybersecurity incidents and
6 known coding vulnerabilities in the industry;
7
8

9 b. Defendant's failure to implement and maintain reasonable security
10 measures also was contrary to legislatively-declared public policy that
11 seeks to protect consumers' data and ensure that entities that are trusted
12 with it use appropriate security measures. These policies are reflected
13 in laws, including the FTC Act (15 U.S.C. § 45), California's Customer
14 Records Act (Cal. Civ. Code § 1798.80 *et seq.*), and California's
15 Consumer Privacy Act (Cal. Civ. Code § 1798.150);
16
17

18 c. Defendant's failure to implement and maintain reasonable security
19 measures also led to substantial consumer injuries, as described above,
20 that are not outweighed by any countervailing benefits to consumers or
21 competition. Moreover, because consumers could not know of
22 Defendant's inadequate security, consumers could not have reasonably
23 avoided the harms that Defendant caused; and
24
25

26 d. Engaging in unlawful business practices by violating Cal. Civ. Code §
27
28

1 1798.82.

2 241. Defendant has engaged in “unlawful” business practices by violating
3
4 multiple laws, including the FTC Act, 15 U.S.C. § 45, and California common law.

5 242. Defendant’s unlawful, unfair, and deceptive acts and practices include:

- 6 a. Failing to implement and maintain reasonable security and privacy
7 measures to protect Plaintiff’s and California Subclass Members’
8 personal information, which was a direct and proximate cause of the
9 Defendant Data Breach;
10
11 b. Failing to identify foreseeable security and privacy risks, remediate
12 identified security and privacy risks, which was a direct and proximate
13 cause of the Defendant Data Breach;
14
15 c. Failing to comply with common law and statutory duties pertaining to
16 the security and privacy of Plaintiff’s and California Subclass
17 Members’ personal information, including duties imposed by the FTC
18 Act, 15 U.S.C. § 45, which was a direct and proximate cause of the
19 Defendant Data Breach;
20
21 d. Misrepresenting that it would protect the privacy and confidentiality of
22 Plaintiff’s and California Subclass Members’ personal information,
23 including by implementing and maintaining reasonable security
24 measures;
25
26
27
28

1 e. Misrepresenting that it would comply with common law and statutory
2 duties pertaining to the security and privacy of Plaintiff's and California
3 Subclass Members' personal information, including duties imposed by
4 the FTC Act, 15 U.S.C. § 45;

6 f. Omitting, suppressing, and concealing the material fact that it did not
7 reasonably or adequately secure Plaintiff's and California Subclass
8 Members' personal information; and

10 g. Omitting, suppressing, and concealing the material fact that it did not
11 comply with common law and statutory duties pertaining to the security
12 and privacy of Plaintiff's and California Subclass Members' personal
13 information, including duties imposed by the FTC Act, 15 U.S.C. § 45.
14

16 243. Defendant's representations and omissions were material because they
17 were likely to deceive reasonable consumers about the adequacy of Defendant's data
18 security and ability to protect the confidentiality of consumers' personal information.
19

20 244. As a direct and proximate result of Defendant's unfair, unlawful, and
21 fraudulent acts and practices, Plaintiff and California Subclass Members were
22 injured and lost money or property, which would not have occurred but for the unfair
23 and deceptive acts, practices, and omissions alleged herein, time and expenses
24 related to monitoring their financial accounts for fraudulent activity, an increased,
25 imminent risk of fraud and identity theft, and loss of value of their personal
26
27
28

1 information.

2 245. Defendant's violations were, and are, willful, deceptive, unfair, and
3
4 unconscionable.

5 246. Plaintiff and California Subclass Members have lost money and
6
7 property as a result of Defendant's conduct in violation of the UCL, as stated herein
8 and above.

9 247. By deceptively storing, collecting, and disclosing their personal
10
11 information, Defendant has taken money or property from Plaintiff and California
12 Subclass Members.

13 248. Defendant acted intentionally, knowingly, and maliciously to violate
14
15 California's Unfair Competition Law, and recklessly disregarded Plaintiff's and
16 California Subclass Members' rights.

17 249. Plaintiff and California Subclass Members seek all monetary and
18
19 nonmonetary relief allowed by law, including restitution of all profits stemming
20
21 from Defendant's unfair, unlawful, and fraudulent business practices or use of their
22
23 personal information; declaratory relief; reasonable attorneys' fees and costs under
24 California Code of Civil Procedure § 1021.5; injunctive relief; and other appropriate
equitable relief, including public injunctive relief.

25 **COUNT V**

26 **Violation of the California Consumer Privacy Act,**
27 **Cal. Civ. Code §§ 1798.100 *et seq.*, § 1798.150(a)**
28 **(On Behalf of Plaintiff and the California Subclass)**

1
2 250. Plaintiff re-alleges and incorporates by reference each and every
3 allegation in this Complaint, as if fully set forth herein.

4 251. The California Consumer Privacy Act (“CCPA”), Cal. Civ. Code §
5 1798.150(a), creates a private cause of action for violations of the CCPA. Section
6 1798.150(a) specifically provides:

8 Any consumer whose nonencrypted and nonredacted personal information, as
9 defined in subparagraph (A) of paragraph (1) of subdivision (d) of Section
10 1798.81.5, is subject to an unauthorized access and exfiltration, theft, or
11 disclosure as a result of the business’s violation of the duty to implement and
12 maintain reasonable security procedures and practices appropriate to the
13 nature of the information to protect the personal information may institute a
14 civil action for any of the following:

15 (A) To recover damages in an amount not less than one hundred dollars
16 (\$100) and not greater than seven hundred and fifty (\$750) per
17 consumer per incident or actual damages, whichever is greater.

18 (B) Injunctive or declaratory relief.

19 (C) Any other relief the court deems proper.

20 252. Defendant is a “business” under § 1798.140(b) in that it is a corporation
21 organized for profit or financial benefit of its shareholders or other owners, with
22 gross revenue in excess of \$25 million.

23 253. Plaintiff and California Subclass Members are covered “consumers”
24 under § 1798.140(g) in that they are natural persons who are California residents.

25 254. The personal information of Plaintiff and the California Subclass
26 Members at issue in this lawsuit constitutes “personal information” under §
27
28

1 1798.150(a) and 1798.81.5, in that the personal information Defendant collects and
2 which was impacted by the cybersecurity attack includes an individual's first name
3 or first initial and the individual's last name in combination with one or more of the
4 following data elements, with either the name or the data elements not encrypted or
5 redacted: (i) Social Security number; (ii) Driver's license number, California
6 identification card number, tax identification number, passport number, military
7 identification number, or other unique identification number issued on a government
8 document commonly used to verify the identity of a specific individual; (iii) account
9 number or credit or debit card number, in combination with any required security
10 code, access code, or password that would permit access to an individual's financial
11 account; (iv) medical information; (v) health insurance information; (vi) unique
12 biometric data generated from measurements or technical analysis of human body
13 characteristics, such as a fingerprint, retina, or iris image, used to authenticate a
14 specific individual.
15
16
17
18
19

20 255. Defendant knew or should have known that its computer systems and
21 data security practices were inadequate to safeguard the California Subclass
22 Members' personal information and that the risk of a data breach or theft was highly
23 likely. Defendant failed to implement and maintain reasonable security procedures
24 and practices appropriate to the nature of the information to protect the personal
25 information of Plaintiff and the California Subclass Members. Specifically,
26
27
28

1 Defendant subjected Plaintiff's and the California Subclass Members' nonencrypted
2 and nonredacted personal information to an unauthorized access and exfiltration,
3 theft, or disclosure as a result of the Defendant's violation of the duty to implement
4 and maintain reasonable security procedures and practices appropriate to the nature
5 of the information, as described herein.
6

7
8 256. As a direct and proximate result of Defendant's violation of its duty,
9 the unauthorized access and exfiltration, theft, or disclosure of Plaintiff's and
10 California Subclass Members' personal information included exfiltration, theft, or
11 disclosure through Defendant's servers, systems, and website, and/or the dark web,
12 where hackers further disclosed the personal identifying information alleged herein.
13

14 257. As a direct and proximate result of Defendant's acts, Plaintiff and the
15 California Subclass Members were injured and lost money or property, including
16 but not limited to the loss of Plaintiff's and California Subclass Members' legally
17 protected interest in the confidentiality and privacy of their personal information,
18 stress, fear, and anxiety, nominal damages, and additional losses described above.
19

20 258. Section 1798.150(b) specifically provides that "[n]o [prefiling] notice
21 shall be required prior to an individual consumer initiating an action solely for actual
22 pecuniary damages."
23

24 259. On October 16, 2023, Plaintiff provided Defendant with written notice
25 of its violations of the CCPA, pursuant to Civil Code § 1798.150(b)(1). If Defendant
26
27
28

1 fails to respond, has not cured, or is unable to cure the violation within 30 days
2 thereof, Plaintiff will amend this Complaint to seek all relief available under the
3 CCPA including damages to be measured as the greater of actual damages or
4 statutory damages in an amount up to seven hundred and fifty dollars (\$750) per
5 consumer per incident. *See* Cal. Civ. Code § 1798.150(a)(1)(A) & (b).
6

7
8 260. Accordingly, Plaintiff and the California Subclass Members by way of
9 this complaint seek actual pecuniary damages suffered as a result of Defendant's
10 violations described herein.
11

12 **COUNT VI**
13 **Violation of the California Customer Records Act,**
14 **Cal. Civ. Code §§ 1798.80 *et seq.***
(On Behalf of Plaintiff and the California Subclass)

15 261. Plaintiff re-alleges and incorporates by reference each and every
16 allegation in this Complaint, as if fully set forth herein.
17

18 262. Cal. Civ. Code § 1798.81.5 provides that “[i]t is the intent of the
19 Legislature to ensure that personal information about California residents is
20 protected. To that end, the purpose of this section is to encourage businesses that
21 own, license, or maintain personal information about Californians to provide
22 reasonable security for that information.”
23

24 263. Section 1798.81.5(b) further states that: “[a] business that owns,
25 licenses, or maintains personal information about a California resident shall
26 implement and maintain reasonable security procedures and practices appropriate to
27
28

1 the nature of the information, to protect the personal information from unauthorized
2 access, destruction, use, modification, or disclosure.”

3
4 264. Cal. Civ. Code § 1798.84(b) provides that [a]ny customer injured by a
5 violation of this title may institute a civil action to recover damages.” Section
6 1798.84(e) further provides that “[a]ny business that violates, proposes to violate, or
7 has violated this title may be enjoined.”
8

9 265. Plaintiff and the California Subclass Members are “customers” within
10 the meaning of Civ. Code § 1798.80(c) and 1798.84(b) because they are individuals
11 who provided personal information to Defendant for the purpose of obtaining a
12 product and/or service, via their employment with Defendant's clients, from
13 Defendant.
14
15

16 266. The personal information of Plaintiff and the California Subclass
17 Members at issue in this lawsuit constitutes “personal information” under §
18 1798.81.5(d)(1) in that the personal information Defendant collects and which was
19 impacted by the cybersecurity attack includes an individual’s first name or first
20 initial and the individual’s last name in combination with one or more of the
21 following data elements, with either the name or the data elements not encrypted or
22 redacted: (i) Social Security number; (ii) Driver’s license number, California
23 identification card number, tax identification number, passport number, military
24 identification number, or other unique identification number issued on a government
25
26
27
28

1 document commonly used to verify the identity of a specific individual; (iii) account
2 number or credit or debit card number, in combination with any required security
3 code, access code, or password that would permit access to an individual's financial
4 account; (iv) medical information; (v) health insurance information; (vi) unique
5 biometric data generated from measurements or technical analysis of human body
6 characteristics, such as a fingerprint, retina, or iris image, used to authenticate a
7 specific individual.
8
9

10 267. Defendant knew or should have known that its computer systems and
11 data security practices were inadequate to safeguard the Plaintiff's and California
12 Subclass Members' personal information and that the risk of a data breach or theft
13 was highly likely. Defendant failed to implement and maintain reasonable security
14 procedures and practices appropriate to the nature of the information to protect the
15 personal information of Plaintiff and the California Subclass Members. Specifically,
16 Defendant failed to implement and maintain reasonable security procedures and
17 practices appropriate to the nature of the information, to protect the personal
18 information of Plaintiff and the California Subclass Members from unauthorized
19 access, destruction, use, modification, or disclosure. Defendant further subjected
20 Plaintiff's and the California Subclass Members' nonencrypted and nonredacted
21 personal information to an unauthorized access and exfiltration, theft, or disclosure
22 as a result of the Defendant's violation of the duty to implement and maintain
23
24
25
26
27
28

1 reasonable security procedures and practices appropriate to the nature of the
2 information, as described herein.

3
4 268. As a direct and proximate result of Defendant's violation of its duty,
5 the unauthorized access, destruction, use, modification, or disclosure of the personal
6 information of Plaintiff and the California Subclass Members included hackers'
7 access to, removal, deletion, destruction, use, modification, disabling, disclosure
8 and/or conversion of the personal information of Plaintiff and the California
9 Subclass Members by the cyber attackers and/or additional unauthorized third
10 parties to whom those cybercriminals sold and/or otherwise transmitted the
11 information.
12
13

14 269. As a direct and proximate result of Defendant's acts or omissions,
15 Plaintiff and the California Subclass Members were injured and lost money or
16 property including, but not limited to, the loss of Plaintiff's and the California
17 Subclass Members' legally protected interest in the confidentiality and privacy of
18 their personal information, nominal damages, and additional losses described above.
19 Plaintiff seeks compensatory damages as well as injunctive relief pursuant to Cal.
20 Civ. Code § 1798.84(b).
21
22
23

24 270. Moreover, the California Customer Records Act further provides: "A
25 person or business that maintains computerized data that includes personal
26 information that the person or business does not own shall notify the owner or
27
28

1 licensee of the information of the breach of the security of the data immediately
2 following discovery, if the personal information was, or is reasonably believed to
3 have been, acquired by an unauthorized person.” Cal. Civ. Code § 1798.82.
4

5 271. Any person or business that is required to issue a security breach
6 notification under the CRA must meet the following requirements under
7 §1798.82(d):
8

- 9 a. The name and contact information of the reporting person or business
10 subject to this section;
11
- 12 b. A list of the types of personal information that were or are reasonably
13 believed to have been the subject of a breach;
14
- 15 c. If the information is possible to determine at the time the notice is
16 provided, then any of the following:
 - 17 i. the date of the breach,
 - 18 ii. the estimated date of the breach, or
 - 19 iii. the date range within which the breach occurred. The notification
20 shall also include the date of the notice;
21
- 22 d. Whether notification was delayed as a result of a law enforcement
23 investigation, if that information is possible to determine at the time the
24 notice is provided;
25
- 26 e. A general description of the breach incident, if that information is
27
28

possible to determine at the time the notice is provided;

f. The toll-free telephone numbers and addresses of the major credit reporting agencies if the breach exposed a social security number or a driver's license or California identification card number;

g. If the person or business providing the notification was the source of the breach, an offer to provide appropriate identity theft prevention and mitigation services, if any, shall be provided at no cost to the affected person for not less than 12 months along with all information necessary to take advantage of the offer to any person whose information was or may have been breached if the breach exposed or may have exposed personal information.

272. Defendant failed to provide the legally compliant notice under § 1798.82(d) to Plaintiff and members of the California Subclass. On information and belief, to date, Defendant has not sent written notice of the data breach to all impacted individuals. As a result, Defendant has violated § 1798.82 by not providing legally compliant and timely notice to all California Subclass Members. Because not all members of the class have been notified of the breach, members could have taken action to protect their personal information, but were unable to do so because they were not timely notified of the breach.

273. On information and belief, many California Subclass Members affected

1 by the breach have not received any notice at all from Defendant in violation of
2 Section 1798.82(d).

3
4 274. As a result of the violations of Cal. Civ. Code § 1798.82, Plaintiff and
5 California Subclass Members suffered incrementally increased damages separate
6 and distinct from those simply caused by the breaches themselves.

7
8 275. As a direct consequence of the actions as identified above, Plaintiff and
9 California Subclass Members incurred additional losses and suffered further harm
10 to their privacy, including but not limited to economic loss, the loss of control over
11 the use of their identity, increased stress, fear, and anxiety, harm to their
12 constitutional right to privacy, lost time dedicated to the investigation of the breach
13 and effort to cure any resulting harm, the need for future expenses and time dedicated
14 to the recovery and protection of further loss, and privacy injuries associated with
15 having their sensitive personal, financial, and payroll information disclosed, that
16 they would not have otherwise incurred, and are entitled to recover compensatory
17 damages according to proof pursuant to § 1798.84(b).

18
19
20
21 **COUNT VII**

22 **Violation of the California Confidentiality of Medical Information Act**
23 **("CMIA"), Cal. Civ. Code § 56, *et seq.***
24 **(On Behalf of Plaintiff and the California Subclass)**

25 276. Plaintiff re-alleges and incorporates by reference each and every
26 allegation in this Complaint, as if fully set forth herein.

27 277. In Section 56.10(a) of the California Civil Code provides that "[a]
28

1 provider of health care, health care service plan, or contractor shall not disclose
2 medical information regarding a patient of the provider of health care or an enrollee
3 or subscriber of a health care service plan without first obtaining an authorization[.]"

5 278. Defendant is a "contractor" within the meaning of Civil Code §
6 56.05(d) within the meaning of Civil Code § 56.06 and/or a "business organized for
7 the purpose of maintaining medical information" and/or a "business that offers
8 software or hardware to consumers . . . that is designed to maintain medical
9 information" within the meaning of Civil Code § 56.06(a) and (b), and maintained
10 and continues to maintain "medical information," within the meaning of Civil Code
11 § 56.05(j), for "patients" of Defendant, within the meaning of Civil Code § 56.05(k).

14 279. Plaintiff and California subclass members are "patients" within the
15 meaning of Civil Code § 56.05(k) and are "endanger[ed]" within the meaning of
16 Civil Code § 56.05(e) because Plaintiff and California subclass members fear that
17 disclosure of their medical information could subject them to harassment or abuse.

20 280. Plaintiff and California subclass members, as patients, had their
21 individually identifiable "medical information," within the meaning of Civil Code §
22 56.05(j), created, maintained, preserved, and stored on Defendant's computer
23 network at the time of the unauthorized disclosure.

25 281. Defendant, through inadequate security, allowed unauthorized third-
26 party access to Plaintiff's and California subclass members' medical information,
27

1 without the prior written authorization of Plaintiff and California subclass members,
2 as required by Civil Code § 56.10 of the CMIA.

3
4 282. In violation of Civil Code § 56.10(a), Defendant disclosed Plaintiff's
5 and California subclass members' medical information without first obtaining an
6 authorization. Plaintiff's and California subclass members' medical information was
7
8 viewed by unauthorized individuals as a direct and proximate result of Defendant's
9 violation of Civil Code § 56.10(a).

10
11 283. In violation of Civil Code § 56.10(e), Defendant further disclosed
12 Plaintiff's and California subclass members' medical information to persons or
13 entities not engaged in providing direct health care services to Plaintiff or California
14 subclass members, or to their providers of health care or health care service plans or
15 their insurers or self-insured employers.

16
17 284. Defendant violated Civil Code § 56.101 of the CMIA through its willful
18 and knowing failure to maintain and preserve the confidentiality of the medical
19 information of Plaintiff and the California subclass members. Defendant's conduct
20 with respect to the disclosure of confidential PII and PHI was willful and knowing
21 because Defendant designed and implemented the computer network and security
22 practices that gave rise to the unlawful disclosure.

23
24
25 285. In violation of Civil Code § 56.101(a), Defendant created, maintained,
26 preserved, stored, abandoned, destroyed, or disposed of Plaintiff's and class
27
28

1 members' medical information in a manner that failed to preserve and breached the
2 confidentiality of the information contained therein. Plaintiff's and California
3 subclass member' medical information was viewed by unauthorized individuals as
4 a direct and proximate result of Defendant's violation of Civil Code § 56.101(a). 380.
5
6 In violation of Civil Code § 56.101(a), Defendant negligently created, maintained,
7
8 preserved, stored, abandoned, destroyed, or disposed of Plaintiff's and California
9 subclass members' medical information. Plaintiff's and California subclass
10 members' medical information was viewed by unauthorized individuals as a direct
11
12 and proximate result of Defendant's violation of Civil Code § 56.101(a).

13 286. Plaintiff's and California subclass members' medical information that
14
15 was the subject of the unauthorized disclosure included "electronic medical records"
16
17 or "electronic health records" as referenced by Civil Code § 56.101(c) and defined
18
19 by 42 U.S.C. § 17921(5).

20 287. In violation of Civil Code § 56.101(b)(1)(A), Defendant's electronic
21
22 health record system or electronic medical record system failed to protect and
23
24 preserve the integrity of electronic medical information. Plaintiff's and California
25
26 subclass members' medical information was viewed by unauthorized individuals as
27
28 a direct and proximate result of Defendant's violation of Civil Code §
56.101(b)(1)(A).

289. Defendant violated Civil Code § 56.36 of the CMIA through its failure

1 to maintain and preserve the confidentiality of the medical information of Plaintiff
2 and the California subclass members.

3
4 289. As a result of Defendant's above-described conduct, Plaintiff and
5 California subclass members have suffered damages from the unauthorized
6 disclosure and release of their individual identifiable "medical information" made
7 unlawful by Civil Code §§ 56.10, 56.101, 56.36. 385.
8

9 290. As a direct and proximate result of Defendant's above-described
10 wrongful actions, inaction, omissions, and want of ordinary care that directly and
11 proximately caused the unauthorized disclosure, and violation of the CMIA, Plaintiff
12 and California subclass members have suffered (and will continue to suffer)
13 economic damages and other injury and actual harm in the form of, inter alia, (i) an
14 imminent, immediate and the continuing increased risk of identity theft, identity
15 fraud and medical fraud-risks justifying expenditures for protective and remedial
16 services for which they are entitled to compensation, (ii) invasion of privacy, (iii)
17 breach of the confidentiality of their PII and PHI, (iv) statutory damages under the
18 California CMIA, (v) deprivation of the value of their PII and PHI, for which there
19 is a well-established national and international market, and/or (vi) the financial and
20 temporal cost of monitoring their credit, monitoring their financial accounts, and
21 mitigating their damages.
22
23
24
25

26 291. Plaintiff, individually and for each member of the California Subclass,
27
28

1 seeks nominal damages of one thousand dollars (\$1,000) for each violation under
2 Civil Code § 56.36(b)(1), and actual damages suffered, if any, pursuant to Civil Code
3 § 56.36(b)(2), injunctive relief, as well as punitive damages of up to \$3,000 per
4 Plaintiff and each California subclass member, and attorneys' fees, litigation
5 expenses and court costs, pursuant to Civil Code § 56.35.
6

7
8 **COUNT VIII**
9 **Common Law Invasion of Privacy – Intrusion Upon Seclusion**
10 **(On Behalf of Plaintiff and the Class)**

11 292. Plaintiff re-alleges and incorporates by reference each and every
12 allegation in this Complaint, as if fully set forth herein.

13 293. To assert claims for intrusion upon seclusion, one must plead (1) that
14 the defendant intentionally intruded into a matter as to which plaintiff had a
15 reasonable expectation of privacy; and (2) that the intrusion was highly offensive to
16 a reasonable person.
17

18 294. Defendant intentionally intruded upon the solitude, seclusion and
19 private affairs of Plaintiff and Class Members by intentionally configuring their
20 systems in such a way that left them vulnerable to malware/ransomware attack, thus
21 permitting unauthorized access to their systems, which compromised Plaintiff's and
22 Class Members' personal information. Only Defendant had control over its systems.
23

24 295. Defendant's conduct is especially egregious and offensive as they
25 failed to have adequate security measures in place to prevent, track, or detect in a
26
27
28

1 timely fashion unauthorized access to Plaintiff's and Class Members' personal
2 information.

3
4 296. At all times, Defendant was aware that Plaintiff's and Class Members'
5 personal information in their possession contained highly sensitive and confidential
6 personal information.

7
8 297. Plaintiff and Class Members have a reasonable expectation of privacy
9 in their personal information, which also contains highly sensitive medical
10 information.

11
12 298. Defendant intentionally configured their systems in such a way that
13 stored Plaintiff's and Class Members' personal information to be left vulnerable to
14 cyber attack without regard for Plaintiff's and Class Members' privacy interests.

15
16 299. The disclosure of the sensitive and confidential personal information of
17 thousands of consumers, was highly offensive to Plaintiff and class members
18 because it violated expectations of privacy that have been established by general
19 social norms, including by granting access to information and data that is private and
20 would not otherwise be disclosed.

21
22 300. Defendant's conduct would be highly offensive to a reasonable person
23 in that it violated statutory and regulatory protections designed to protect highly
24 sensitive information, in addition to social norms. Defendant's conduct would be
25 especially egregious to a reasonable person as Defendant publicly disclosed
26
27
28

1 Plaintiff's and Class Members' sensitive and confidential personal information
2 without their consent, to an "unauthorized person," i.e., hackers.
3

4 301. As a result of Defendant's actions, Plaintiff and Class Members have
5 suffered harm and injury, including but not limited to an invasion of their privacy
6 rights.
7

8 302. Plaintiff and Class Members have been damaged as a direct and
9 proximate result of Defendant's intrusion upon seclusion and are entitled to just
10 compensation.
11

12 303. Plaintiff and class members are entitled to appropriate relief, including
13 compensatory damages for the harm to their privacy, loss of valuable rights and
14 protections, and heightened stress, fear, anxiety, and risk of future invasions of
15 privacy.
16

17 **PRAYER FOR RELIEF**

18 WHEREFORE, Plaintiff prays for judgment as follows:
19

20 A. For an Order certifying this action as a class action and appointing
21 Plaintiff and his counsel to represent the Class and California
22 Subclass;
23

24 B. For equitable relief enjoining Defendant from engaging in the
25 wrongful conduct complained of herein pertaining to the misuse
26 and/or disclosure of Plaintiff's and Class Members' Private
27
28

1 Information, and from refusing to issue prompt, complete and
2 accurate disclosures to Plaintiff and Class Members;

3
4 C. For equitable relief compelling Defendant to utilize appropriate
5 methods and policies with respect to consumer data collection,
6 storage, and safety, and to disclose with specificity the type of Private
7 Information compromised during the Data Breach;

8
9 D. For injunctive relief requested by Plaintiff, including but not limited
10 to, injunctive and other equitable relief as is necessary to protect the
11 interests of Plaintiff and Class Members, including but not limited to
12 an order:

13
14 i. Prohibiting Defendant from engaging in the wrongful and
15 unlawful acts described herein;

16
17 ii. Requiring Defendant to protect, including through encryption,
18 all data collected through the course of its business in
19 accordance with all applicable regulations, industry standards,
20 and federal, state, or local laws;

21
22 iii. Requiring Defendant to delete, destroy, and purge the Private
23 Information of Plaintiff and Class Members unless Defendant
24 can provide to the Court reasonable justification for the
25
26
27
28

1 retention and use of such information when weighed against
2 the privacy interests of Plaintiff and Class Members;

3
4 iv. Requiring Defendant to implement and maintain a
5 comprehensive Information Security Program designed to
6 protect the confidentiality and integrity of the Private
7 Information of Plaintiff and Class Members;
8

9 v. Prohibiting Defendant from maintaining the Private
10 Information of Plaintiff and Class Members on a cloud-based
11 database;
12

13 vi. Requiring Defendant to engage independent third-party
14 security auditors/penetration testers as well as internal security
15 personnel to conduct testing, including simulated attacks,
16 penetration tests, and audits on Defendant's systems on a
17 periodic basis, and ordering Defendant to promptly correct any
18 problems or issues detected by such third-party security
19 auditors;
20

21
22 vii. Requiring Defendant to engage independent third-party
23 security auditors and internal personnel to run automated
24 security monitoring;
25
26
27
28

- viii. Requiring Defendant to audit, test, and train its security personnel regarding any new or modified procedures;
- ix. Requiring Defendant to segment data by, among other things, creating firewalls and access controls so that if one area of Defendant's network is compromised, hackers cannot gain access to other portions of Defendant's systems;
- x. Requiring Defendant to conduct regular database scanning and securing checks;
- xi. Requiring Defendant to establish an information security training program that includes at least annual information security training for all patients, with additional training to be provided as appropriate based upon the patients' respective responsibilities with handling personal identifying information, as well as protecting the personal identifying information of Plaintiff and Class Members;
- xii. Requiring Defendant to routinely and continually conduct internal training and education, and on an annual basis to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach;

1 xiii. Requiring Defendant to implement a system of tests to assess
2 its respective patients' knowledge of the education programs
3 discussed in the preceding subparagraphs, as well as randomly
4 and periodically testing patients' compliance with Defendant's
5 policies, programs, and systems for protecting personal
6 identifying information;

7
8
9 xiv. Requiring Defendant to implement, maintain, regularly review,
10 and revise as necessary a threat management program designed
11 to appropriately monitor Defendant's information networks for
12 threats, both internal and external, and assess whether
13 monitoring tools are appropriately configured, tested, and
14 updated;

15
16
17 xv. Requiring Defendant to meaningfully educate all Class
18 Members about the threats that they face as a result of the loss
19 of their confidential personal identifying information to third
20 parties, as well as the steps affected individuals must take to
21 protect themselves; and

22
23
24 xvi. Requiring Defendant to implement logging and monitoring
25 programs sufficient to track traffic to and from Defendant's
26 servers; and
27
28

xvii. for a period of 10 years, appointing a qualified and independent third party assessor to conduct a SOC 2 Type 2 attestation on an annual basis to evaluate Defendant's compliance with the terms of the Court's final judgment, to provide such report to the Court and to counsel for the Class, and to report any deficiencies with compliance of the Court's final judgment.

E. For equitable relief requiring restitution and disgorgement of the revenues wrongfully retained as a result of Defendant's wrongful conduct;

F. Ordering Defendant to pay for not less than ten years of credit monitoring services for Plaintiff and the Class;

G. For an award of actual damages, compensatory damages, statutory damages, and statutory penalties, in an amount to be determined, as allowable by law;

H. For an award of punitive damages, as allowable by law;

I. For an award of attorneys' fees and costs, and any other expense, including expert witness fees;

J. Pre- and post-judgment interest on any amounts awarded; and

K. Such other and further relief as this court may deem just and proper.

JURY TRIAL DEMANDED

1 Plaintiff demands a trial by jury on all claims so triable.
2

3 Dated: October 16, 2023

Respectfully submitted,

4 s/ John J. Nelson

5 John J. Nelson (SBN 317598)

6 **MILBERG COLEMAN BRYSON**

7 **PHILLIPS GROSSMAN, LLC**

8 280 S. Beverly Drive

9 Beverly Hills, CA 90212

10 Telephone: (858) 209-6941

11 Fax: (858) 209-6941

12 Email: jnelson@milberg.com

13 *Attorney for Plaintiff and*
14 *the Proposed Class*
15
16
17
18
19
20
21
22
23
24
25
26
27
28